redsquid.

Redsquid.
Managed Services

1 Contents

2 Definitions

In this Agreement, the following left side terms have the meanings ascribed opposite to them:

Term	Meaning
The Company	Redsquid
The Customer	As referenced in the associated contract.
The System	All supported items as referred to in support items.
Third-Party Software	All software not covered in the support items.
Updates	A revision of a version. For example, updating from revision 10.1 to 10.2 where 10 is the version and .2 is the update.
Upgrades	A new version. For example, upgrading from version 10.3 to 11.0 where 11 is the version.
Payment	The transfer of money from Customer to The Company.
Ticket Logged	The recording of a Customer's request for assistance.
Ticket Logging Window	The times at which the Customer can log tickets.
SLA	The agreed amount of time within which The Company will respond verbally or digitally to the Customer, within the ticket logging window.
SLA Timer	A timer that defines how much time has passed since the ticket has been raised, within the ticket logging window.
Chargeable	A piece of work that will be charged to the Customer, at a pre-agreed on fee, payable in 30 days from date of invoice.
Support Service	Access to our support team on the basis defined in support service.
Installation	The provisioning of new or additional hardware or software.
Reconfiguration	The adjustment of settings on already provisioned software or the reallocation of hardware already provisioned.
Work	Any undertaking by an engineer on the Customer's behalf.
Account Balance	The total monetary value of invoices yet to be paid.
Out of hours	Any time outside of the ticket logging window.
The vendor	Manufacturer of the software.

Migration/s	Moving a service/system/software from one physical or digital location to another.
Service termination date	The date after which services are no longer contracted, paid for or delivered.

3 Payment

The Company may invoice one month ahead of time for services. For example, services that run from August 1st will be invoiced on July 1st. The Customer will pay the invoice within 30 days of it being issued.
Use of the Company's direct debit scheme, Go Cardless, is mandatory for paying for all services.
If payment is not made of any sum due to The Company by the due date, The Company reserves the right to withhold all services and collect any associated hardware, until such sum is paid in full. In addition, interest shall become payable at the rate of 4% above Barclays Bank plc base rate for time being in force until such payment is made. Additional interest and compensation pursuant to the Late Payment of Commercial Debts (Interest) Act 1997 may be charged at the Company's discretion.

All charges billed will be quoted for and agreed verbally or digitally with the Customer before work is undertaken. This work is subject to sign off from authorised site contacts.

All sums payable under this agreement unless otherwise stated are exclusive of VAT and other duties or taxes. Any VAT or other duties or taxes payable in respect of such sums shall be payable in addition to such sums.

If you, the Customer, receive a request via email to make any changes to your account or to transfer funds other than to the Company's Go Cardless account, you must not make any payment or respond to the email and must contact The Company immediately.

4 IT Service Desk Service

5 Service Description

The Company's helpdesk service provides technical support to the Customer, as detailed below.
The Company may store information relating to your IT setup, in its secure database ITGlue. This database is protected with MFA.
We partner with Uptime Solutions to augment our support service with a 24/7 offering. We also use Uptime Solutions for over flow support. To facilitie this relationship they have access to ITGlue.

6 Company Obligations

7 Ticket Logging Methods

The Company will provide access to ticket logging by one or more methods below, during the ticket logging window:

- Telephone – 020 1866 4540
- Email – itsupport@redsquid.co.uk
- Software Agent – RMM

Tickets may not be logged directly with the engineers via email or Teams.

8 Ticket Logging Window

The Customer may log tickets between the hours of 8:00 am and 6.00 pm weekdays, excluding public holidays.
Logging tickets outside of this window can be done in the following ways:

- Telephone – leaving a voicemail.

- Email
- Software Agent

Tickets logged outside of this window will not be responded to until the start of the next ticket logging window.

9 Service Level Agreements (SLAs)

The Company operates the following SLAs:

- 1 hour – Critical priority
- 2 hour – High priority
- 4 hour – Medium priority
- 8 hours – Low priority

SLAs are defined by The Company. The Customer may not define the priority but can request it be adjusted, at the discretion of The Company.
Priorities are defined as follows:

- **Critical** – Inability for the Customer's business to function at all and where no workaround is possible.
- **High** – Inability for an individual within the Customer's business to function at all and where no workaround is possible. This will normally be caused by workstation failure but will not be affecting any other users.
- **Medium** – Any issue where a workaround is possible or a solution is not necessary immediately.
- **Low** – All other issues.

10 Support Location

Support is provided remotely. Onsite visits for support are chargeable.

11 Supported Items

Supported items details the list of items that The Company will spend an unlimited amount of time fixing, without additional charge.
If this solution requires a specialist to repair or replace goods, then the costs incurred will be passed back to the Customer if outside the manufacturer's warranty period.
If under warranty, any delivery or returns costs incurred will be passed onto the Customer.
Time spent on any items not listed below will be considered chargeable.
The following items are covered by the support service:

- Microsoft Windows and Apple client operating systems that are within the vendor's support lifecycle, as defined by the vendor.
- Windows and Apple client OS roles and features that are within the support vendor's lifecycle, as defined by the vendor.
- Microsoft Server operating systems that are within the vendor's support lifecycle, as defined by the vendor.
- Microsoft Server roles and features that are within the vendor's support lifecycle, as defined by the vendor.
- Microsoft Exchange within the vendor's support lifecycle, as defined by the vendor.
- Microsoft Office within the vendor's support lifecycle, as defined by the vendor.
- Remote Access – PPTP VPN, L2TP VPN, SSL VPN, RDP (Remote Desktop), Direct Cloud.

- Branded workstation, laptop and server hardware – only the time taken to pinpoint a hardware issue is covered, the replacement of hardware and the time associated with that replacement are not covered by the support service.
- Backup Software – Only backup software sold by The Company is supported.
- File restores – Only for supported backup software, subject to backup sign off form.
- Routers
- Hubs and switches
- Firewalls
- Exclaimer
- Screens
- Docking stations
- Printer software
- Scanner software
- Uninterruptable Power Supplies
- Cabling
- Internet Connectivity – ADSL, FTTC, FTTP, 3G, 4G, Leased Line
- PSTN Line
- Panda Antivirus
- Domain names – Provided the domain is hosted with the Company's chosen provider.
- Consultancy - To provide an advisory service to the Customer on any matter concerning supported items.

12 Unsupported Items

If an item is not on the supported items list above then the item is not covered by The Company's help desk service. For further clarity, some unsupported items are specifically listed, but not limited to the below.

- Windows and Apple endpoints without The Company's RMM agent installed.
- Office / Microsoft 365 – Microsoft 365 is not covered by the support service and is covered by a separate service.
- Microsoft products outside of their support life cycle, as defined by Microsoft.
- Client workstation hardware older than seven years.
- Microsoft Windows Server Backup – This is always deemed insufficient to protect business data therefore excluded from the support service.
- Root cause analysis – The Company will undertake such root cause analysis as they deem necessary in order to comply with their obligations under this agreement. Further root cause analysis requested by the Customer maybe chargeable at the Company's absolute discretion.
- Breach Remediation
- Hardware built from components ordered from separate vendors.
- Laptop, workstation and server hardware upgrades or replacements.
- Changes to signature templates within Outlook or Exclaimer.
- Microsoft SQL
- Website migrations and amendments
- iOS and Android and any non-Microsoft apps that run on them
- Hosted VoIP or On-premise phone systems – unless expressly agreed between the parties.
- Printer hardware

- Cyber security consultation – the helpdesk will react to security breaches under the contract but this does not include Cyber security planning or Security audits
- Server rebuild or restore
- BCDR – Business continuity and disaster recovery planning are not covered under the help desk service.
- Reports and documentation – The Company will create documentation and reports for internal use only. If the Customer requires reports or documentation creating, this maybe chargeable.

If the Customer requests help with unsupported items such assistance will incur additional charges.

13 Out of hours work

The Company will conduct support outside of business hours; this work will incur additional charges.

14 Personal Computers

Personal computers are supported only at the absolute discretion of The Company and will only be treated as Low priority.
The Company will endeavour to provide support for personal computers that are required to connect to systems covered by the service contract. The scope of this support is limited to providing successful connectivity to the covered system. If the source of any problem lies with personally owned hardware or software then The Company reserves the right to charge the Customer for the work necessary to restore the service.

15 Third-Party Software (Representative Support)

The Company does not directly support third party application software. Third party software is defined as all software not covered in the in support items.
The Company will only provide representative support for third party software with the permission of the Customer.
Representative support is defined as The Company liaising with the provider or support representative of the third party software to facilitate a solution.
In all instances where third party support is required, The Company requires the Customer to first contact the third party support provider for help. If the issue is not resolved the name or reference number of the supporting engineer must then be passed to The Company, who will make a reasonable effort to contact the third party support provider to facilitate a solution. The Company will not be liable for any failure to affect a solution.

16 Industry updates and notifications

The Company will endeavour to keep the Customer informed of new software & hardware releases, updates, and other developments in our opinion pertinent to the Customer's business, although The Company cannot be held responsible if such information is not communicated.

17 Updates, Upgrades, Installations, Reconfiguration and Migrations

Updates, upgrades, installation, reconfiguration and migrations of software or hardware as defined in definitions will be deemed chargeable by The Company.
The Company will endeavour to carry out this work at time which is mutually convenient. This work is not covered by the support service SLA's.

18 Software "How To"

Limited to ensuring that the software works without generating errors or crashing. "How to" functionality is not covered by the service contract. Training can be provided on a

chargeable basis.

19 Customer Obligations

20 Site Contact

The Customer must have one or more site contacts who are readily available to coordinate and authorise work. This site contact does not have to be technically trained but needs to act as a conduit between the Company and the Customer.
The Customer must ensure that all site contacts have the required time and authority to implement the recommendations made by The Company.

21 Third Party Software

The Company requires that the Customer's site contact has sufficient knowledge of third party software, so as to provide first line support to their internal users.

22 Backups

The Customer is responsible for ensuring that adequate backups of their system are made and tested, unless otherwise agreed with the Company in the corresponding backup sign off form.
The Company will proactively advise and assist the Customer to put an adequate backup procedure in place but ultimately the Customer is responsible for ensuring that adequate backups are taken.
The Customer is required to review and sign a backup sign off form mutually agreed by the Customer and The Company.

23 Adherence to Advice

The Company cannot be held responsible for the Customers failure to implement reasonable, industry standard, advice.

24 Licensing

The Customer is responsible for tracking, storing and documenting all licences and software, whether purchased through The Company or directly from other suppliers.
The Customer shall provide The Company with access to the above information to enable The Company to carry out the terms of this Contract. If the Customer fails to provide such information, the Company reserves the right to levy additional charges if work is restricted due to the unavailability of these items.

25 Security

The Customer is responsible for ensuring that all best-practice security measures are in place. The Company will endeavour to advise the Customer upon these measures but liability for the consequences of a security breach lies with the Customer.

26 Patch Management

27 Service Description

Patch management will be applied to covered devices and will attempt to roll out authorised Microsoft and Apple patches. These patches will be applied weekly, typically on a Thursday. Patches are not always applied correctly, this is due to operating system issues with Microsoft and Apple. The Company will make best endevours to contact the users of affected devices to resolve patch deployment issues.

28 Professional Services

29 Service description

The Company can provide professional services at an documented hourly rate. The goal of these services will be agreed before the work is undertaken, and a time estimate provided where reasonably possible.
For Customers who do not have a help desk service contract, credit card details or upfront payment is required.
Work will be billed for whole hours only, at the following rates:
1st line engineer - £90 per hour
2nd line engineer - £110 per hour
3rd line engineer - £135 per hour
These rates may be subject to change at any time.
An engineer of a suitable level will be recommended, but The Customer can request a higher tier engineer.
It is not always possible to achieve the project goal in the amount of time estimated. Once the estimated time has been reached, sign off for further time will be requested before moving forward.
While The Company takes all measures to prevent additional problems occurring, sometimes These do occur and the time spent upon resolving additional issues will be charged at the engineer's usual hourly rate as set out above.

30 Expedited Service or Fast Tracking

The Company will offer an expedited service for one-off installations of certain types of equipment and services, for an additional fee. The expedited service will entitle the Customer to have the hardware/software within a 3 day period from date of delivery.

31 Microsoft 365 (M365)

32 Service Description

The Company will provide M365 services as detailed below.

33 Company Obligations

34 Support Delivery

Support will be delivered as described in here.

35 Supported Items

The Company will only support M365 products that are provided by The Company. If the Customer procures their M365 licensing elsewhere then support may not be provided.
The Company endeavours to support the following items within the M365 platform:

- Office – The Company will support Office to the point that it opens, advanced feature support, as defined by the Company, is not provided.
- Exchange Online
- SharePoint Online
- OneDrive
- Teams
- Business Voice
- Forms

36 Customer Obligations

37 Backup

Both The Company and Microsoft recommend that M365 be augmented with an additional third-party backup service. The built-in backup functionality within M365 is not deemed sufficient for business needs by The Company and The Company cannot be held liable for loss of data that occurs when additional backups are not in place.

38 Licensing

It is the Customer's responsibility to manage their user licensing and inform The Company if licenses are no longer required. Access to the M365 admin portal can be made available upon request.
The Company may automatically add licenses as needed to provision new user setups.

39 Managed Backup Services

40 Service Description

The following backup solutions, when provided by The Company, are managed backup services:

- SaaS Backup / Backupify / M365 Backup
- Cloudberry
- TOD Extra
- TOD Lite

41 Company Obligations

42 Monitoring

The Company will check "managed" backups each day and digitally record if the backup has been a success or failure.
If the backup has failed The Company will attempt to remedy the backup within three business days. If a solution has not been found the Customer will be notified on the fourth day.

43 Backup Sign Off Form

The backup sign off form is a critical document. The aim of this document is to provide clarity between the Company and the Customer about the backup solution in place. This includes, but is not limited to, the following information:

- Managed Service – yes or no
- Systems/items backed up
- Schedule
- Backup software
- Onsite and offsite storage location
- Retention – refers to how long backups are kept for before being purged.
- Versioning – refers to the number of revision of a file/server are kept.
- Granular – refers to the ability to be able to restore individual items, not just the whole server.
- Backup fitness – is the backup sufficient for business needs?
- What data is backed up, when and to where.

No other form of communication, written or verbal, may supersede this document.
The Company will provide this document to the Customer.
The Company cannot be held responsible for the loss of any data that is not listed on the backup sign off form.

44 Data Access

All full time qualified engineers at The Company have access to the Customer's backup data. This data will only be accessed when a restore has been requested.

45 Security

Data will be encrypted in transit and at rest.
Once a backup service has been cancelled, all Customer data will be removed from the Company's systems, no later than one month after the cancellation date. No data restores will be available after this point.

46 Support Delivery

Support will be delivered via email, telephone or video.

47 Customer Obligations

48 Test Restores

The Company advises that the Customer requests test restores. The frequency of these test restores should be in line with The Customers BCDR plan. The Company cannot be held responsible for data restores, should test restores not been requested by The Customer.

49 SaaS Backups

When an employee of the Customer leaves their employ, their data will continue to be backed up until such time as the Customer notifies The Company that they explicitly want the data to be removed from the backup Service.

50 Backup Sign Off Forms

The Customer is required to sign the Company's backup sign off form. The Customer is required to keep a copy of The Company's backup sign off form. This form includes all details about the specification of the backup. The Company cannot be held responsible for data restores, should a signed backup sign off form not be in place.
The Customer is responsible for making sure that The Company is aware of business critical data which needs backing up if it is not on the backup sign off form.

51 TOD Extra - Managed Disaster Recovery Backup

52 Service Description

TOD Extra is a managed backup and disaster recovery service that takes regular image backups of included Customers services onsite and offsite. The Service is only deployed on Customer request and is appropriate for on premise data primarily on file servers.

The Company will check for successful backups each day and conduct weekly test restores of data only. Full disaster recovery tests can be completed but are only done upon Customer request.

A description of what, when and to where the backups take place can be found on the Customers copy off the backup sign off form.

Backups are encrypted at rest and in transit. Onsite media is password protected and onsite backup images are encrypted by Blowfish encryption. Offsite media is encrypted by Microsoft BitLocker and images are encrypted with Blowfish encryption.

Data will be stored offsite in the Company's Thame data centre. Data access is only permitted to authorised engineers, and a strict and immediate engineer offboarding policy is in place.

Recovery times are estimated at 7 GB per hour, and The Company endeavours to provide a loan server for the duration of a server recovery period. The recovery period lasts for 30 days only. The recovery period starts from the time that the Customer and The Company agree that a recovery should be initiated. If the loan server is required for additional time

additional charges may be levied.

Once the TOD Extra service has been cancelled, all data will be removed from The Company's systems with immediate effect.

53 Company Obligations

54 Support Delivery
Support will be delivered as described in here.

55 Backup failure remediation
A backup failure will be diagnosed with the highest level of priority. If a backup failure is not resolved in 2 business days the ticket will be escalated to a senior engineer. If the backup failure has not been resolved for 7 days then a manager/director will be informed and the Customer notified.

56 TOD Lite – Managed Disaster Recovery Backup

57 Service Description

TOD lite is a managed backup and disaster recovery solution for Windows client computers.

58 Company Obligations

59 Support Delivery
Support will be delivered as described in here.

60 Backup failure remediation
A backup failure will be diagnosed with the highest level of priority. If a backup failure is not resolved in 2 business days the ticket will be escalated to a senior engineer. If the backup failure has not been resolved for 7 days then a manager/director will be informed and the Customer notified.

61 Retention and versioning
The below bullet points explain how long backups will be stored for.

- Keep all intra-daily backups for 7 days.
- After that, keep daily backups for the next 1 week.
- After that, keep weekly backups for the next 1 month.
- Keep the remaining backups for 1 year.

62 Data Destruction
Once this service has been cancelled, all data will be removed from the Company's platform by the day after the last billing period. Once data has been deleted, there will be no option to restore, and this process is irreversible.

63 Website Hosting Services

64 Service Description
The Company will provide a platform to host websites. This will only be deployed on Customer requests.

65 Company Obligations

66 Support Delivery
Support will be delivered via email only.

67 Supported Items
The Company will ensure that the platform is digitally accessible from a working internet connection.

68 Unsupported Items
The Company is not responsible for fixing a broken website when the website hosting platform is accessible. The Company recommends that the Customer seeks the advice of a website development consultant.
The Company is not responsible for ongoing website maintenance or amendments.

69 Security
Data is stored with our trusted third party provider on their secure platform. The Company is not responsible for the data y stored by the Customer on this platform.

70 Managed Rental

71 Service Description
A managed equipment rental includes hardware, software and support. Only some offerings are considered managed rentals. If the Customer is unsure if they have a managed rental, they should contact their account manager.

72 Equipment Refresh
Managed rental hardware is subject to an equipment refresh on the schedule agreed in the signed contract. Pricing for the Service may change at this time.

73 Support Delivery
Support will be delivered as described in here.

74 Supported Items
For the life of the term, as detailed in the managed rental contract, The Company will provide help and support for the following items:

- Hardware and Software – for items rented as part of the managed rental. The Company will make a reasonable effort to provide a next business day replacement for any hardware that has failed.
- Firmware updates

75 Cabling

76 Service description
Cabling is the installation and/or ongoing connectivity of physical cables by The Company or a contractor authorised by The Company.

77 Company Obligations

78 Warranty
The Company will warrant cabling installations for a period of three months from the date of installation. The Company will only warrant natural degradation of parts and correct problems directly caused by the installation.
The Company offers a four week resolution SLA.

79 TTL Cloud General

80 Service description
TTL Cloud relates to the following services:

- Hosted Exchange Email
- Hosted Remote Desktop Services
- Dedicated Servers
- Virtual Private Servers (VPS)

81 Security

82 Administrative Access
Each engineer with infrastructure level access to TTLCloud has their own login and can be separately audited.

All manufacturer default hardware and software logins are changed before deployment.

All administration level accounts on the TTLCloud require regular password resets and conform to industry standard password complexity requirements.

A principle of least privilege is applied when assigning rights.

Administrative access to TTL Cloud is audited.

83 Data Location
All data is stored within the EEA (European Economic Area), however The Company reserves the right to store data outside the UK as required.

84 Encryption
All data is encrypted at rest using AES 128-bit encryption. Encryption keys are stored in an encrypted database.

85 Perimeter Security

The perimeter of the TTL Cloud network is protected by a firewall which only allows traffic to and from its intended sources.

86 Offboarding

Unused infrastructure and software is removed within one month of it becoming obsolete.

Engineer access is revoked immediately upon an engineer leaving the Company's employ.

87 Data Destruction

Hard disks and servers are digitally and physically destroyed in an industry standard way.

88 Antivirus

It is The Company's responsibility to make sure up to date antivirus and antimalware software is installed on all endpoints.

89 System Patches

Security updates and patches will be regularly applied to all endpoints.

90 Physical Security

Physical access to systems within the TTLCloud are restricted to personnel who explicitly need access rights to complete a task.

24 hour CCTV is in place in all data centres.

91 User Level Security

The Company is not responsible for a data breach caused by the use of insecure passwords on the TTL Cloud network. The definition of what constitutes a secure password may change in accordance with standard industry practices and guidelines.

14.2.11 Tenancy Separation

Where appropriate The Company will ensure that Customer data is only accessible by the Customer who is authorised to do so.

92 Data Protection

The Company has taken all reasonable measures to protect personal data stored on the TTLCloud.

Appropriate security measures have been implemented to prevent accidental or deliberate compromise of personal data.

It is the responsibility of the Customer to review the risks associated with storing data on TTL Cloud.

The Company reserves the right to immediately remove, without warning, data breaking criminal or civil laws.

There may be times when data is passed to a trusted third party. The Company reserves the right to do this on the basis that it is done only for problem resolution. All third parties are trusted associates of The Company.

Data access is monitored by The Company and access activity auditable. Data access is restricted to key Company personnel of The Company who will ensure that the data is treated as sensitive, protected and not divulged to any unauthorised third parties.

93 Termination

Data will be permanently removed from The Company's systems 30 days after the Customer provides written cancellation of their Service.

The Company ensures that data will be made available to authorised individuals for extraction from the TTL Cloud network, but only up until the service cancellation date. If data is required after this date access may incur additional charges.

If the Customer requires The Company to extract data on their behalf then extra charges may be incurred for this process and for any shipping and transmission required as a consequence of it..

94 Monitoring

The Company monitor up time of hardware and software and act on this in accordance with their service level agreements.

95 Maintenance

The Company reserves the right to perform quarterly maintenance on the TTL Cloud infrastructure. This maintenance may require up to one day of downtime.

The Company reserves the right to update vendor software on the TTL Cloud network in order to ensure the security and stability of the platform.

96 Acceptable Use Policy

97 Internet Abuse

You, the Customer, may not use the Company's network to engage in illegal, abusive, or irresponsible behaviour, including:

1.1 unauthorised access to or use of data, Services, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorisation of the owner of the system or network;

1.2 monitoring data or traffic on any network or system without the authorisation of the owner of the system or network;

1.3 interference with Service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;

1.4 use of an Internet account or computer without the owner's authorisation;

1.5 collecting information by deceit, including, but not limited to Internet scamming

(tricking other people into releasing their passwords), password robbery, phishing, security hole scanning, and port scanning;
1.6 use of any false, misleading or deceptive TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting;
1.7 use of the Service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
1.8 any activity or conduct that is likely to result in retaliation against the Company's network;
1.9 any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations including data protection;
1.10 introducing intentionally or knowingly into the Service any virus or other contaminating program or fail to use an up to date virus-scanning program on all material downloaded from the Services;
1.11 sending unsolicited e-mails ("spam");
1.12 misrepresenting yourself as other computer networks and users; or
1.13 any activity or conduct that unreasonably interferes with our other Customers' use of our Services.

98 Bulk Commercial E-Mail

2.1 You the Customer may not use The Company's Cloud to send bulk mail. Please see the applicable Product Terms and Conditions for those Services. You may use your dedicated hosted system to send bulk mail, subject to the restrictions in this Acceptable Use Policy
2.2 Under the European Directive 2002/58/CE of 12 July 2002 on privacy and electronic communications, the use of e-mail for direct marketing is only allowed to recipients who have given their prior consent. The Company acknowledges that market research is not considered as direct marketing within the meaning of the Directive above, and therefore, the requirements set out below do not apply to bulk e-mails for market research purposes. You must obtain The Company's advance approval for any bulk commercial e-mail other than for market research purposes, for which you must be able to demonstrate the following to The Company's reasonable satisfaction:
2.2.1 Your intended recipients have given their consent to receive e-mail via some affirmative means, such as an opt-in procedure;
2.2.2 Your procedures for soliciting consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which the consent is given;
2.2.3 You retain evidence of the recipient's consent in a form that may be promptly produced within 72 hours of receipt of recipient's or The Company's requests to produce such evidence;
2.2.4 The body of the e-mail must include information about where the e-mail address was obtained, for example, "You opted in to receive this e-mail promotion from our Web site or from one of our partner sites," and information on how to request evidence of the consent, for example, "If you would like to learn more about how we received your email address please contact us at abuse@yourdomain.com";
2.2.5 You have procedures in place that allow a recipient to revoke their consent – such as a link in the body of the e-mail, or instructions to reply with the word "Remove" in the subject line, and such revocations of consent are implemented within 72 hours;2.2.6 You must post an abuse@yourdomain.com e-mail address on the first page of any Web site associated with the e-mail, you must register that address at abuse.net, and you must promptly respond to messages sent to that address;
2.2.7 You must have a Privacy Policy posted for each domain associated with the mailing;
2.2.8 You have the means to track anonymous complaints;
2.2.9 You may not obscure the source of your e-mail in any manner. Your e-mail must

include the recipient's e-mail address in the body of the message or in the "TO" line of the e-mail.
2.3 These policies apply to messages sent using your The Company Cloud Service or network, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site hosted via your The Company Cloud Service. You may not use third party e-mail services that do not have similar procedures for all its Customers.
2.4 The Company may test and monitor your compliance with these requirements, including requesting opt-in information from a random sample of your list at any time.

99 Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a The Company Cloud system or network or to breach The Company's security or authentication measures, whether by passive or intrusive techniques without The Company's prior written consent.

100 Offensive Content

4.1 You may not publish, display or transmit via The Company's network and equipment any content that The Company reasonably believes:
4.1.1 constitutes or encourages child pornography or is otherwise obscene, sexually explicit or morally repugnant;
4.1.2 is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
4.1.3 is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
4.1.4 is defamatory or violates a person's privacy;
4.1.5 creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement bodies;
4.1.6 improperly exposes trade secrets or other confidential or proprietary information of another person;
4.1.7 is intended to assist others in defeating technical copyright protections;
4.1.8 infringes another person's trade or service mark, patent, or other property right;
4.1.9 is discriminatory in any way, including by way of sex, race, or age discrimination;
4.1.10 facilitates any activity or conduct that is or may be defamatory, pornographic, obscene, indecent, abusive, offensive or menacing;
4.1.11 involves theft, fraud, drug-trafficking, money laundering or terrorism;
4.1.12 is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to The Company; and
4.1.13 is otherwise malicious, fraudulent, or may result in retaliation against The Company by offended viewers.
4.2 Content "published or transmitted" via The Company's network or equipment includes Web content, e-mail, bulletin board postings, chat, and any other type of posting, display or transmission that relies on the Internet.

14.6.5 Export Control

The Services may not be used by persons, organisations, companies or any such other legal entity or unincorporated body, including any affiliate or group Company, which violates export control laws (including in any manner which would constitute a breach of Section 8 of the General Terms and Conditions) and/or is:
5.1 involved with or suspected of involvement in activities or causes relating to:

5.1.1 illegal gambling;
5.1.2 terrorism;
5.1.3 narcotics trafficking;
5.1.4 arms trafficking or the proliferation of weapons of mass destruction;
including any affiliation with others whatsoever who sponsor or support the above such activities or causes.

14.6.6 Copyrighted Material

6.1 You may not use The Company's network or equipment to download, publish, distribute, or otherwise copy in any manner any text, music, software, art, image or other work protected by copyright law unless:
6.1.1 you have been expressly authorised by the owner of the copyright for the work to copy the work in that manner; and
6.1.2 you are otherwise permitted by copyright law to copy the work in that manner.
6.2 The Company will terminate the Service of copyright infringers in accordance with the HSA.

14.6.7 Cooperation with Investigations and Legal Proceedings

7.1 The Company may monitor any content or traffic belonging to you or to users for the purposes of ensuring that the Services are used lawfully. The Company may intercept or block any content or traffic belonging to you or to users where Services are being used unlawfully or not in accordance with this AUP and you do not stop or provide The Company with an acceptable reason within 7 days of receipt of a formal written notice from The Company.
7.2 The Company e may, without notice to you:
7.2.1 report to the appropriate authorities any conduct by you that The Company reasonably believes violates applicable law, and
7.2.2 provide any information The Company has about you, or your users or your traffic and cooperate in response to a formal or informal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil action that on its face meets the requirements for such a request.
7.3 If The Company is legally required to permit any relevant authority to inspect your content or traffic, you agree The Company can provide this where possible without breaching any legal or regulatory requirement you are given reasonable prior notice of such requirement and an opportunity to oppose and/or attempt to limit such inspection in each case to the extent reasonably practicable.

14.6.8 Shared Systems

You may not use any shared system provided by The Company Cloud in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, The Company may prohibit the automated or scripted use of The Company Cloud Mail Services if it has a negative impact on the mail system or may require you to repair coding abnormalities in your Cloud-hosted code if it unnecessarily conflicts with other Cloud Customers' use of the Cloud. You agree that The Company may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the system or other Customers' data that is stored on the same system.

14.6.9 Other

9.1 You must have valid and current information on file with your domain name registrar for any domain hosted on our network.
9.2 You may only use IP addresses assigned to you by The Company's staff.

9.3 You may not take any action which directly or indirectly results in any of The Company's IP space being listed on any abuse database.
9.4 You agree that if you register a DNS record or zone on The Company Cloud managed or operated DNS servers or services for a domain of which you are not the registrant or administrative contact according to the registrars WHOIS system, that, upon request from the registrant or administrative contact according to the registrars WHOIS system, The Company Cloud may modify, transfer, or delete such records or zones.

14.6.10 Consequences of Violation of terms of service

You are strictly responsible for the use of your The Company Cloud Service in breach of this AUP, including use by your Customers, and including unauthorised use that you could not have prevented. The Company will charge you our standard hourly rate for work on any breach of the AUP together with the cost of equipment and material needed to:
10.1 investigate or otherwise respond to any suspected violation of this AUP;
10.2 remedy any harm caused to us or any of our Customers by the use of your Service in violation of this AUP;
10.3 respond to complaints; and
10.4 have our Internet Protocol numbers removed from any "blacklist".

14.6.11 Disclaimer

The Company is under no duty, and by this AUP are not deemed to undertake a duty, to monitor or police our Customers' activities and we disclaim any responsibility for any misuse of our network.

101 Backups

Information about how your backups are handled can be found on your backup sign off form. If you do not have a backup sign off form, please enquire with The Company.

102 SLA

The TTL Cloud SLA is 99% uptime for unplanned failures.
Our systems are monitored 24 hours a day and fixes are carried out between 8 – 9.30 weekdays.

The Company will not be liable or responsible for any failure to perform, or delay in performance of, any of our obligations under the Contract that is caused by events outside our reasonable control ("Force Majeure Event").

103 Hosted Remote Desktop

104 Service Description

The Company provides Hosted Remote Desktop services to its Customers, stored within its Thame data centre.

105 Company Obligations

User level access is not audited.

106 Support delivery

Support will be delivered via email, telephone or video.

107 Customer Obligations

The Customer is responsible for the licensing and support of any non-Microsoft software on the Cloud network.

The Customer is responsible for ensuring they are using secure passwords

108 Dedicated Servers

109 Service Description

Dedicated servers provide the Customer with a physical server, hosted in the cloud, used only by the Customer.

110 Company Obligations

111 Deployment Time Frame

The Company agrees to deploy the Customer's dedicated infrastructure within 14 days of a signed order form. Servers are deemed deployed once connection information has been handed over to the Customer.

112 Support delivery

Support will be delivered as described in here.

113 Supported Items

Supported items detail the list of items that The Company will spend an unlimited amount of time fixing, without charge, to the point where the business need is met.
Time spent on any items not listed under support cover will be considered chargeable.
The following items will be supported:

- Server hardware
- Server operating system
- Ensuring the system is online and available for access

114 Unsupported Items

- Software installations
- Software reconfiguration

115 Unsupported Configuration

If The Company is asked to implement a configuration element (hardware or software) or hosting Service in a manner that is not customary for The Company, or that is in "end of life" or "end of support" status then The Company may designate the element or Service as "unsupported", "non-standard", "best efforts", "reasonable endeavours", "one-off", "EOL", "End of Support". The Company makes no representation or warranty whatsoever regarding unsupported Service so designated, and the Customer agrees that The Company shall not be liable for any loss or damage arising from the provision of the unsupported Service. The SLA shall not apply to the Unsupported Service, or any other aspect of the Hosting Services that is adversely affected by the Unsupported Service. The Customer acknowledges that Unsupported Services may not interoperate with The Company's other services, such as backup or monitoring.

116 Security

It is the Customer's responsibility to encrypt any sensitive data that is stored or transferred to and from their dedicated server. The Company will encrypt the hardware but it is The Customer's responsibility to encrypt data in transit and at rest.

117 Data Destruction

Once the Customer's contract has ended all data will be removed from The Company's systems within 30 days. Data can be copied to media provided by the Customer and will be in VHD or VHDX format only.

118 IP Addressing

WAN IP addresses associated with the Customer's dedicated server belong to The Company and at termination of the Service these IP addresses are non-transferable.

119 Customer Obligations

120 Licensing

The core operating system will be licensed by The Company, but the Customer is responsible for the cost of additional software required.

121 Resale and 3rd Party Access

The Customer may resell the Hosting Services, subject to the provisions of Section 15 of the General Terms and Conditions. If the Customer resells any part of the Hosting Services they must require their Customers sign a written contract that includes the following:

An acknowledgement that such Customer will abide by The Company's terms of Service and shall have no right of action against The Company in connection with the dedicated server service that is being resold.
A prohibition against high risk use of the hosting services: "No High Risk Use. You may not use the hosting services in any situation where failure or fault of the hosting services could lead to death or serious bodily injury of any person, or to physical or environmental damage. For example, you may not use, or permit any other person to use, the hosting services in connection with aircraft or other modes of human mass transportation, nuclear or chemical facilities, or medical life support devices."
The Company is not responsible for any contract with the 3rd party in question and any claims or agreements made within.

122 Backup

It is the responsibility of the Customer to ensure that key data is backed up on dedicated servers. If you are unsure please see your backup sign off form.

123 CyberSafe

124 Service Description

CyberSafe provides a combination of the following technologies and services, as listed in your signed contract:

- MDR

- SOC
- SIEM
- Consultation
- Security Assessment and Vulnrability Scanning
- Security Roadmap
- Executive Risk Report
- Dark Web Scanning
- End User Security Policy
- End User Security Tarining
- Attack Simulations

CyberSafe makes best endevours to secure your IT infrastructure but cannot guarantee that a breach will not occur. Redsquid cannot take any responsibility for the consequences of a breach.
A Customer contact is required to co-oridate Customer resources for all CyberSafe technologies and services.
Consultation hours:

- Consultation hours can be used for any security related activity.
- Consultation hours cant be carried over from year to year.
- Additional hours can be purchased upon request.

Incident response:

- Incident response uses your consultation hours.
- An incident response manager will be assigned to you from the point you are breached, till all our recommend remediation steps are completed. Providing this is within your consultantion hours.
- Incident response manager hours are 9 - 5:30 weekdays.
- An written incident response report will be provided after each incident.
- It is the responsibility of the Customer to notify the ICO. Redsquid recommend the ICO is always notified if a breach occurs.

SOC:

- All SOC activity is audited.
- SOC SLA's:
  Urgent Priority - 1 hour
  High Priority - 2 hours
  Medium Priority - 4 hours
  Low Priority - 8 Hours
- SOC activity is out sourced to our partner ConnectWise

125 Microsoft Azure

126 Service Description

Microsoft Azure is provided "as is" direct from Microsoft with the addition of supported items detailed below.

127 Supported Items

- The Company will ensure that the Azure service instance is running and available to connect to.

128 Unsupported Items

- VPS operating systems – This may be covered by by your service desk service.
- Azure security and compliance queries – This maybe covered by your security or CyberSafe contract.

129 Trifi

Trifi support is remote only, onsite support is chargeable.

130 General

131 Force Majeure

The Company shall be relieved from all liabilities, under any contract, to the extent that it shall be unable to perform all or any of the obligations thereunder by reasons of war, strikes, lockouts, government controls, act of God, restrictions, non-availability of goods or personnel or any cause whatsoever beyond the control of The Company.

132 Privacy and GDPR

The Company treats Customers' data seriously, details of this can be found on The Company's website -

133 Applicable Law

The agreement to which these conditions applies shall be subject to and construed in accordance with the law of England and Wales and the Senior Court of England and Wales shall have exclusive jurisdiction over the enforcement and interpretation of his agreement.

134 Call Recording

The Company records all incoming and outgoing calls to its switchboard in compliance with GDPR lawful data processing under legitimate interest.

135 Consequential Loss

The Company is not liable for the Customer's loss of profit or any other consequential loss including loss of business.

136 Virus, Malware or Malicious Damage

The Company is not liable for damage caused by malicious actions from physical or digital threats of any kind, regardless of how the threat infiltrated the system.

137 Customers without a help desk service

For Customers without a help desk service, The Company reserves the right to deliver support for its other services via email only.

138 Delivery and Courier

The Company are not responsible for damage or loss of items shipped to and from their offices or associated offices.