SPECIFIC CONDITIONS J1 – CONNECTIVITY SERVICES

These Specific Conditions govern the Connectivity Services that may be provided by the Company under an Order Form, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms & Conditions for the Supply of Products and/or Services (the "**Conditions**") and Specific Conditions X3 – Standard Operational Services ("**Specific Conditions X3**"), which shall be deemed to be incorporated into the Contract for the performance of any Connectivity Services performed under these Specific Conditions.

The Connectivity Services set out under the headings "Internet Access", "Point to Point Leased Line Services", "WAN Connectivity Services", "Managed Services", "Cloud Connectivity Services" and/or "DDP Services" shall only benefit the Customer to the extent such Services are referred to as being part of this Contract in the Order Form.

1 DEFINITIONS

1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions only.

"ADSL"	means an asymmetric digital subscriber line, which is a type of circuit connection that allows for higher Downstream Bandwidth and lower Upstream Bandwidth;
"AF Class"	means assured forwarding, for delay-sensitive data traffic;
"Allowable Parked Time"	means where an Incident is 'parked' (on hold) while the Company, the Carrier and/or the Service Provider is seeking further information and/or access from the Customer in order to resume investigation and/or resolution of the Incident once the information or access is received;
"Available"	means as defined and calculated in accordance with paragraph 24;
"Bandwidth"	means an amount of data traffic measured in b/s (bits per second) across the inter-connect;
"BE Class"	means best-effort, for traffic that is not AF Class or EF Class;
"Broadband Acceptable Use Policy"	means the Company's policy for the acceptable use of its Broadband Services and/or the internet, the current version of which is available at www.daisyuk.tech (or at such other website address as is notified to the Customer by the Company from time to time);
"Broadband Services"	means the provision of a connection to the internet for the Customer supplied through the Company Network utilising xDSL, FTTC, SOADSL, SOGEA, FTTP and/or G.fast technologies in accordance with paragraph 7.1;
"Cellular Internet Access"	means the Services detailed in paragraph 7.3;
"Cloud Connectivity Services"	means, if specified in the Order Form, the connection for the Customer to the Customer's cloud service provider as detailed in paragraph 13;
"Co-Management Services"	means the Services delivered to the Customer in accordance with paragraph 12.12;
"Company Network"	means the backbone connectivity infrastructure owned, managed and maintained by the Company that interconnects with other Service Provider and Carrier infrastructures to provide the Connectivity Services;
"Connection Date"	means the date when the Service Provider, having received the relevant information from the Company, is in a position to and has agreed to commence provision of the Connectivity Services to the Customer, as notified to the Customer;
"Connectivity Services"	means the Services provided under these Specific Conditions, as specified in the Order Form;
"CPE"	means customer premises equipment, being the edge router or device that, where applicable, sits immediately behind the Network Termination Equipment;
"Customer Provided Apparatus"	means any apparatus at the Customer Premises (not being Services Equipment) provided and used by the Customer and/or an End User in order to use the Connectivity Services;
"DDoS Attack"	means a denial of service attack, which is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services consuming the Bandwidth of the Connectivity Services or otherwise overloading the resources of the Connectivity Services;
"DDP Services"	means the Services provided in accordance with paragraph 14;
"Demarcation Point"	means where the Connectivity Services terminate at the Customer Premises, as defined in paragraph 10.3.3, 10.4.2 or 10.7 as applicable;
"Dedicated Management Platform"	means a dedicated software build of the Fortinet Inc management platform either within the Company's shared infrastructure or on Customer Premises;
"Downstream"	means the transmission of data from the Company Network to the Customer;
"EF Class"	means expedited forwarding, for IP Voice applications;
"Ethernet"	means a connection with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems, including but not limited to GEA, EoFTTC, EoFTTP and EFM;
"EFM"	means an Ethernet circuit connection within the "first mile" from the Customer's Premises to the Network, although from the Carrier's point of view it is known as the "last mile";
"EoFTTC"	means an Ethernet connection over FTTC;
"EoFTTP"	means an Ethernet connection over FTTP;
"FortiAnalyzer"	means software provided by Fortinet Inc;
FortiManager"	means software provided by Fortinet Inc;
"Fibre Ethernet"	means a dedicated, private, fixed capacity Ethernet circuit connection;
"FTTC"	means fibre infrastructure to the nearest cabinet to the Customer Premises;
"FTTP"	means fibre infrastructure to the Customer Premises;
"GEA"	means generic Ethernet access, which is an entry-level form of Ethernet connectivity that harnesses copper technology between the Customer Premises and the cabinet and then fibre to the exchange, before handing data over to the Ethernet network;
"G.fast"	means 330Mbps capable hybrid fibre "ultrafast broadband" ISP technology, which is a form of FTTC;
"Internet Access"	means Broadband Services and/or Managed Internet Access;
"IP"	means internet protocol, which is the method or protocol by which data is sent from one computer to another on the internet;
"IP Address"	means internet protocol address, which is the unique identifier for a computer or other device that distinguishes it from all other devices connected to the internet;
"Intrusion Prevention System (IPS)"	means a network security tool that monitors a network for malicious activity and takes action to help to prevent it;
"Jitter"	means the variation or difference in the end-to-end delay between received packets of data in an IP packet stream, measured as the average difference in one way delay between successive test packets during a calendar month;
"Latency"	means the average one-way data packet transmission time measured in milliseconds between the Demarcation Point and the first PoP in the Company Network;

"Managed Fortinet SD-WAN Overlay"	means, if specified in the Order Form, the services as detailed in paragraph 12;
"Managed Internet Access"	means the Services provided in accordance with paragraph 7.2;
"Managed Equipment"	means any CPE or other equipment that is listed in the Order Form as Managed Equipment for the purposes of these Specific Conditions;
"Management Platform"	means a software build of the Fortinet Inc management platform which may be syndicated or dedicated to the Customer as specified on the Order Form;
"Measurement Period"	means as defined in paragraph 24;
"MPLS"	means multi-protocol label switching, which is a mechanism for routing traffic within a WAN as data travels from one network node to the next;
"Network"	means any part of the end to end connectivity within the Carrier or Service Provider's network used to facilitate Connectivity Services that interconnects with the Company Network but is not owned or under the control of the Company;
"Network Termination Equipment"	means any network termination equipment (together with the software embodied within it) provided by or utilised by the Company and/or Service Provider at the end of the circuit connection to the Customer Premises to provide a data connection from the CPE to the Network;
"Packet Loss"	means the percentage of packets of data travelling across a network that fail to reach their destination, and is calculated as an average of all test packets sent and received in one month';
"Planned Outages"	means any Connectivity Services downtime: i. scheduled by the Company to carry out any preventative or other maintenance services as notified to the Customer; or ii. caused by any upgrade services in relation to the Connectivity Services or the Company's systems, which the Customer has or has not requested, as notified to the Customer; or iii. caused by any Service Requests or Changes approved by the Customer including without limitation, redesign or reconfiguration of the Connectivity Services;
"Point to Point Leased Line Service"	means a Fibre Ethernet leased line provided by the Company in accordance with paragraph 9;
"PoP"	means point-of-presence, which is an access point from one place within the Company Network, the Network or the internet to another;
"PSTN"	means a public switched telephone network, which uses circuit-switched copper phone lines to transmit analogue voice data;
"QoS Service Class"	means quality of service, being a type of IP configuration used to define the service class type of the packets of data travelling across a network (as either voice, video, mission critical data or standard class data);
"SD-WAN"	means software-defined networking in a WAN, which is a network architecture approach that enables a WAN to be intelligently and centrally controlled or programmed using software applications and which therefore simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism;
"SD-WAN Overlay Asset Management"	means the services delivered to the Customer in accordance with paragraph 12.5;
"SD-WAN Overlay IPS Reporting "	means the services delivered to the Customer in accordance with paragraph 12.9;
"SD-WAN Overlay Monitoring and Event Management"	means the services delivered to the Customer in accordance with paragraph 12.2;
"SD-WAN Overlay Monthly Health Reporting"	means the services delivered to the Customer in accordance with paragraph 12.6;
"SD-WAN Overlay Reactive Technical Support"	means the services delivered to the Customer in accordance with paragraph 12.3;
"SD-WAN Overlay Review Meeting"	means the services delivered to the Customer in accordance with paragraph 12.8;
"SD-WAN Overlay Security Review Meeting"	means the services delivered to the Customer in accordance with paragraph 12.10;
"SD-WAN Overlay Security Updates"	means the services delivered to the Customer in accordance with paragraph 12.4;
"Security Update"	means a firmware update that is released by the Vendor to address a security related issue;
"Service Availability"	means the calculation of time that the Connectivity Services are Available in accordance with paragraph 22;
"Service Provider"	means any third party telecommunications service provider from whom the Company procures services in order to provide the Connectivity Services under this Contract;
"Services Equipment"	means any apparatus, equipment and cabling including but not limited to the Network Termination Equipment provided by the Company (and/or the relevant Carrier and/or Service Provider) at a Customer Premises as an essential part of providing the Connectivity Services under the terms of this Contract, which shall remain the property of the Company and/or the relevant Carrier and/or Service Provider;
"Service Contention"	means where there is more than one customer sharing the same Bandwidth in the underlying Network;
"SIM Card"	means subscriber identity modules to enable access to network services;
"SOGEA"	means a single order GEA, delivered as a single service using copper technology between the Customer Premises and the cabinet and then fibre to the exchange, where the line is not shared with PSTN;
"SOADSL"	means a single order transitional access product, delivered as a single service using copper technology between the Customer Premises and the cabinet, where the line is not shared with PSTN;
"Statement of Works"	means the Order Form or any other relevant contractual document setting out the scope of services as referred to in the Order Form;
"Syndicated Management Platform"	means a software build of the Fortinet Inc management platform within the Company's shared infrastructure;
"Unavailable"	means the time that the Connectivity Services are not available as calculated in accordance with paragraph 23;
"Upstream"	means the transmission of data from the Customer to the Company Network;
"Uptime"	means the amount of time that the Connectivity Services at the Customer Premises is online, available and operational;
"Virus"	means any type of malware, virus, worm, Trojan horse, ransomware, spyware, adware, scareware or other computer program or software code that has been introduced into a computer, system or network that carries out a useless and/or destructive function

	such as displaying an irritating message or systematically over-writing the information stored (that is, "infect" them) and spreads by contact between an infected program and an uninfected program;
"WAN"	means a wide area network, which is a telecommunications network or computer network that extends over a large geographical distance;
"Wires Only"	means provision of the connectivity only within a WAN, with no managed element provided by the Company, as provided in accordance with paragraph 10.3; and
"xDSL"	means ADSL and/or DDSL.

1.2 All other capitalised terms that are not defined in paragraph 1.1 shall have the meanings stated in the Conditions, Specific Conditions X3 or other applicable Specific Conditions.

2 MINIMUM TERM

2.1 The Minimum Term for the Connectivity Services is as set out in the Order Form, or if no Minimum Term is specified, twelve (12) calendar months from and including the Connection Date.

3 PROVISION OF CONNECTIVITY SERVICES

3.1 The Company will use reasonable endeavours to provide the Connectivity Services from the Connection Date subject to these Specific Conditions. The Connectivity Services may not be fault free and use of the Connectivity Services may not be uninterrupted.

3.2 Subject to the continuing supply of the service by the relevant Carrier and/or Service Provider, in the event of a fault occurring in the Connectivity Services the Company will use reasonable endeavours to rectify the fault as soon as practicable. The Company shall have no liability to the Customer for any fault occurring or any interruption to the Connectivity Services whether in contract, tort (including without limitation negligence or breach of statutory duty) or otherwise to the extent caused by any act or omission by the relevant Carrier and/or Service Provider or any known or unknown Viruses.

4 USE OF CONNECTIVITY SERVICES

4.1 The Customer is responsible for the safe custody and safe use by it of the Connectivity Services and without prejudice to the generality of the foregoing the Customer agrees and undertakes:

4.1.1 not to cause any Customer Provided Apparatus, other than those that meet the requirements of any Relevant Laws, to be connected to the Connectivity Services and the Company shall not be under any obligation to connect or keep connected any Customer Provided Apparatus if it does not so conform or if in the reasonable opinion of the Company it is liable to cause death, personal injury or damage or to impair the quality of the Connectivity Services;

4.1.2 to use the Connectivity Services in accordance with Relevant Laws and in a manner that does not cause the Company to breach any Relevant Laws;

4.1.3 not to use the Connectivity Service in a manner that constitutes a violation or infringement of the rights (including, without limitation, any Intellectual Property Rights) of any other person;

4.1.4 to implement adequate control and security over the use of the Connectivity Services provided to the Customer, including but not limited to the prevention of Viruses and/or any calls generated by rogue diallers or hackers; and

4.1.5 not to use the Connectivity Services to send or procure the sending of any bulk unsolicited advertising or promotional material or in a manner that is in any way fraudulent or in bad faith or that has any fraudulent or bad faith purpose or effect.

4.2 All Services Equipment installed or provided by or on behalf of the Company for the purposes of providing the Connectivity Services shall at all times remain the property of the Company and shall be returned to the Company immediately upon request following the termination of this Contract. The Customer shall be liable to the Company for all losses, costs and expenses incurred by the Company for the recovery, replacement or repair of such Services Equipment (save to the extent that the same is caused by the negligence of the Company).

4.3 The Connectivity Services are provided solely for the Customer's use and the Customer may not resell or attempt to resell the Connectivity Services (or any part of them) to any third party. In addition, if the Customer has a mail server, the Customer must not allow relay emails from outside its domain from the Customer's mail server.

4.4 Neither the Customer nor any other person may use the Connectivity Services in any way to send, receive or store any material that could constitute or encourage conduct that would be considered a criminal offence or that is either offensive, abusive, indecent, obscene, pornographic, fraudulent, libellous, defamatory, menacing, criminal or likely to cause annoyance or distress to any third party or likely to incite or promote illegal activities in any jurisdiction.

4.5 Both parties agree to fully co-operate with the Police and any other relevant authorities (including but not limited to HM Revenue and Customs, Trading Standards, the Information Commissioner and/or OFCOM and their successors from time to time) in connection with any misuse or suspected misuse of the Connectivity Services, and the Customer consents to the Company co-operating with any such authority and with any other telecommunications operators in connection with any misuse or suspected misuse or suspected fraudulent activity related to or connected with the Connectivity Services and agrees, without prejudice to the generality of the foregoing, that the Company will be entitled to divulge any information that the Company holds that may be relevant to any investigation, including the name, address and account information relating to the Customer to such third parties.

4.6 To prevent spam from entering and affecting the operation of the Company's systems and the Connectivity Services, the Company may, but is not obliged to, take any reasonable measures or actions necessary to block access to, or delivery of, any e-mail that appears to be of an unsolicited nature and/or part of a bulk e-mail transmission. The Company may also but is not obliged to unless otherwise expressly provided under this Contract, use Virus screening technology that may result in the deletion or alteration of e-mails and or e-mail attachments. The Company shall have no liability whether in contract, tort (including without limitation negligence and breach of statutory duty) or otherwise if the Virus screening technology is not completely effective in any way, including (without limitation) against unsolicited emails or against any Viruses.

4.7 The Customer will comply with the Broadband Acceptable Use Policy to the extent relevant to its use of the Connectivity Services. The Company may change the Broadband Acceptable Use Policy at any time by publishing the changes on its website (www.daisyuk.tech or at such other website address as is notified to the Customer by the Company from time to time) 30 (thirty) days before the change is to take effect.

4.8 In respect of FTTC, SOADSL and SOGEA, the Bandwidth stated is based on the "peak Upstream" rate declared by the Carrier as being available at time of order and may be subject to variation due to copper line quality or other factors outside of the direct control of the Company.

4.9 Unless otherwise agreed in writing by the Company the Connectivity Services must not be used to make or receive any type of telephone/fax calls at any time. The Customer acknowledges that the Connectivity Services are not designed to be a carrier interconnect service and the Customer agrees not to connect diallers of any description or any other telephony equipment to the Connectivity Services.

5 MIGRATION FROM THIRD PARTIES

5.1 Where the migration of lines and services from third party suppliers is selected by the Customer in the Order Form, then the provision of any and all relevant existing services supplied to the Customer by such third party supplier will be migrated to the Company and charged by the Company in accordance with the relevant Charges from the Commencement Date.

5.2 The Customer and not the Company shall be liable for any charges (including without limitation any early termination charges) made by third party suppliers for any migration or transfer of lines and services or otherwise, unless it is clearly identified and agreed in writing in the Order Form as the Company's responsibility.

5.3 If the Customer is migrating to the Broadband Services from a third party provider of an alternative broadband service, the Customer will need to obtain a Migration Authorisation Code ("MAC") from that service provider and provide it to the Company in sufficient time to process the Customer's migration. The Company will not be liable for any delay, costs, expenses, loss or damage arising through failure to connect the Customer to the Broadband Services as a result of the Customer's failure to provide the MAC as required by this paragraph.

6 FRAUD AND SECURITY

6.1 Save as provided in the remainder of this paragraph 6, the Company shall not be responsible for call charges or other charges resulting from fraudulent and/or unauthorised use of the Connectivity Services or any use of the Connectivity Services by any unauthorised third parties (who are not employees of the Company), and the Customer shall be responsible for all use of the Connectivity Services in association with the Customer's accounts whether or not authorised by the Customer. The Customer agrees to immediately notify the Company of any unauthorised use of the Customer's account of which the Customer becomes aware and the Customer agrees to pay all additional charges related to fraudulent and/or unauthorised usage.

6.2 The Customer shall ensure that user names and passwords used by it and/or its personnel and/or End Users in connection with the Connectivity Services are kept secure and confidential at all times and are only used by authorised users. The Customer shall inform the Company immediately if the Customer knows or suspects that a user name or password has been disclosed to an unauthorised user, or is being used in an unauthorised way, or if there is any illegal, fraudulent or unauthorised use of the Connectivity Services or Supported Equipment.

6.3 The Company reserves the right (at the Company's sole discretion):

6.3.1 to suspend access to the Connectivity Services for one or more End Users if at any time the Company thinks that there has been or is likely to be a breach of security (including a breach of the Customer's obligations under this paragraph 6); and

6.3.2 to require the Customer to (in which case, the Customer shall) change any or all of the passwords that the Customer uses in connection with the Connectivity Services.

6.4 The Customer accepts and acknowledges that the Connectivity Services are not guaranteed to be secure and the Company does not guarantee the prevention or detection of any unauthorised attempts to access the Connectivity Services. The Customer shall remain responsible for the security and firewalls of the Customer's communications links, equipment, software, services and processes used in connection with the Connectivity Services unless expressly agreed otherwise in this Contract or in writing by the Company.

6.5 Any assistance given by the Company in relation to fraudulent and/or authorised use by the Customer or third parties (or the prevention of such use) of the Connectivity Services will be on an endeavours basis only and no liability can be accepted by the Company for any loss sustained by the Customer via fraudulent and/or unauthorised means that are beyond the Company's reasonable control (save for any fraud and/or authorised use by an employee of the Company acting in that capacity).

7 INTERNET ACCESS

7.1 **Broadband Services**

7.1.1 The Broadband Services will be provided by the Company to those Customer Premises stated in the Order Form for Broadband Services. Except where otherwise expressly stated in the Order Form, the Broadband Services do not include the provision of any modems or other Services Equipment.

7.1.2 The Customer acknowledges that, in order to use the Broadband Services, the Customer needs an existing telephone line (if not expressly agreed to be provided by the Company under this Contract) and a personal computer of a minimum specification suitable for the Broadband Services. The Customer is responsible for ensuring that compatible cables and extension leads are used to and from its telephone sockets, modems and personal computers in order to use the Broadband Services.

7.1.3 In circumstances where the Customer receives only the Broadband Services from the Company, the Customer remains responsible for making payment to the Customer's fixed line telephony services provider for all rental charges relating to the Customer's relevant telephone line (together with any repair and maintenance charges) and all call charges from the Customer's fixed line telephony service provider.

7.1.4 For the avoidance of doubt, the actual bandwidth speed available is not guaranteed and will depend on a number of factors, including but not limited to: the distance from the exchange; the quality and availability of a copper line, contention rates, extreme weather and any external electrical interference from outside sources.

Unmanaged Broadband Services

7.1.5 Unless identified in the Order Form that the Company will provide Managed Equipment, it will;

(a) provide delivery of the CPE to a location determined by the Customer;

(b) provide delivery of replacement CPE where the hardware is deemed faulty; and

(c) preconfigure the CPE with basic configuration to enable it to connect to the Broadband Services and include installation directions (where applicable).

7.1.6 Unless identified in the Order Form that the Company will provide Managed Equipment, there shall be no expectation on the Company to provide any software or configuration support at any time.

Managed Broadband Services

7.1.7 Where identified in the Order Form that the Company will provide Managed Equipment, it will;

(a) provide delivery of the CPE to a location determined by the Customer;

(b) the CPE will be preconfigured with basic configuration to enable it to connect to the Broadband Services and include installation directions (where applicable); and

(c) provide software and configuration support by telephone.

7.1.8 All CPE provided as part of the Broadband Services, whether as part of a managed or unmanaged Broadband Service is Services Equipment for the purposes of this Contract.

7.2 **Managed Internet Access**

7.2.1 The Managed Internet Access will be provided by the Company from the Company Network to those Customer Premises stated in the Order Form for Managed Internet Access. Except where otherwise expressly stated in the Order Form, the Managed Internet Services do not include the provision of any modems or other Services Equipment.

7.2.2 Where stated in the Order Form that the Company is providing Managed Internet Access, it will include:

(a) the access option(s) stated in the Order Form: GEA, EoFTTC, EoFTTP, EFM or Fibre Ethernet (leased line); and

(b) the corresponding Bandwidths.

7.2.3 The Managed Internet Access may share infrastructure with the Company Network and/or that of other Service Providers.

7.2.4 Where identified in the Order Form that the Company will provide Managed Internet Access, it will;

(a) provide delivery of the CPE to a location determined by the Customer;

(b) the CPE will be preconfigured with basic configuration to enable it to connect to the Managed Internet Access and include installation directions (where applicable); and

(c) provide software and configuration support by telephone.

7.2.5 The Managed Internet Access will also include a break-out for general access to the internet, unless otherwise agreed.

7.2.6 Any new circuit connection will be installed in accordance with the details set out in the Order Form and in accordance with Special Conditions X8 – Installation Services.

7.3 **Cellular Internet Access**

7.3.1 This paragraph 7.3 will only apply where stated in the Order Form that the Company is providing Cellular Internet Access. The terms and conditions set out in Specific Conditions M3 – Daisy Multi Network IOT Services will apply in addition to these Specific Conditions where the Company is providing a Data Only Connection (as defined in Specific Conditions M3 – Daisy Multi Network IOT Services) to the Customer as part of the Cellular Internet Access. In the event of any conflict between this paragraph 7.3 and Specific Conditions M3 – Daisy Multi Network IOT Services, this paragraph 7.3 will take precedence.

7.3.2 Cellular Internet Access will include:

(a) a Data Only Connection (unless stated otherwise in the Order Form);

(b) CPE; and

(c) Incident Management support.

7.3.3 The Minimum Term for Cellular Internet Access is as set out in the Order Form, or if no Minimum Term is specified, twelve (12) months from and including the date on which a Data Only Connection is established, or where the Customer has opted to use its own SIM card or fixed line connectivity pursuant to paragraph 7.3.4, the date on which such connection is established (the "**Cellular Internet Access Minimum Term**"). After expiry of the Cellular Internet Access Minimum Term, Cellular Internet Access will continue on a rolling monthly basis. Either party may terminate the Cellular Internet Access by giving to the other party not less than forty five (45) days' prior written notice to expire on or at any time after expiry of the Cellular Access Minimum Term.

7.3.4 Where the Customer has opted to use its own SIM card or fixed line connectivity instead of the Data Only Connection, the Company will at the initial set-up, provide optimisation configuration. Any additional optimisations requested by the Customer will be available at the Company's sole discretion and will be subject to an additional charge of £200.00 (two hundred pounds) per configuration. Such charge will be paid by the Customer in clear funds prior to the configuration taking place. The Customer accepts and acknowledges that there may be limitations as to the level and/or nature of optimisation that the Company is able to perform. The Customer accepts that if the Company is not able to perform the optimisation to the standard required by the Customer, the Customer shall not be entitled to a refund of any optimisation configuration charge paid by the Customer.

7.3.5 In the event that the Customer raises an Incident Notification, it shall, at the time of raising the Incident, provide the following information to the Service Desk:

(a) details of the affected site(s), including the post code;

(b) a clear and accurate description of the Incident giving rise to the fault;

(c) the time the fault occurred:

(d) confirmation of whether the Incident is persistent;

(e) a description of how power at the site is monitored and checked;

(f) confirmation that there is power feeding into the CPE and/or connected routers;

(g) confirmation as to whether the CPE has been re-booted and if so, the time and result;

(h) the affected number of users; and

(i) any photographs of the affected CPE that may assist the Company with troubleshooting the Incident.

7.3.6 The Company will not be responsible for, or liable to the Customer for any cessation of, or for any loss or disruption to connectivity and any data that arises in relation to any connection provided by a third party supplier or telecommunication services operator, including (but not limited to) where such third party connection is connected to a CPE.

7.4 **General**

7.4.1 The Internet Access may be used by the Customer to link into third party websites, services, resources or networks worldwide. The Company does not accept responsibility for such third party content nor endorses such content. The Customer agrees to comply with the terms and conditions and acceptable use policies of such websites, services, resources and networks. When making use of the Internet Access, the Customer agrees that:

(a) all visual, textual or other information, whether publicly posted or privately transmitted is the sole responsibility of the person from whom such information originated;

(b) it is entirely responsible for all information uploaded, downloaded, emailed or otherwise transmitted via the Internet Access;

(c) all dealings with, and interests in, third party promotions, services or merchants found by the Customer using the Internet Access, are solely between the Customer and the third party with whom the Customer is dealing; and

(d) access to secure financial transactions will be dependent on third party hardware and the third party supplier of content.

7.4.2 The Customer acknowledges that the speed of any Internet Access depends on a number of factors including, but not limited to, distance from the exchange, local availability and line capability. The Company shall have no liability to the Customer whether in contract, tort (including without limitation negligence or breach of statutory duty) or otherwise if the Customer's line does not produce the maximum speed advertised or otherwise referred to.

7.4.3 The Customer acknowledges that the Internet Access is provided from infrastructure that is shared by other users and the Company owes a duty to these users as a whole to preserve its network integrity and avoid network degradation. If, in the Company's reasonable opinion, the Company believes that the Customer's use of the Internet Access is in breach of the Broadband Acceptable Use Policy or otherwise has or may adversely affect such network integrity or may cause network degradation, the Company may change the Customer's chosen access rate or manage the Customer's Internet Access as the Company sees fit in the circumstances.

8 EQUIPMENT

8.1 Any equipment connected to the Connectivity Services by the Customer must be:

8.1.1 technically compatible with the Connectivity Services and not harm the Company Network, the Connectivity Services, the Services Equipment or any third party's network or equipment;

8.1.2 connected and used in line with any relevant instructions or standards including, in the order of precedence set out below:

(a) any legal requirements imposed upon the parties including requirements arising from General Condition 2 set under section 45 of the Communications Act 2003;

(b) any relevant specification notified by OFCOM in implementation of the recommendations of the Network Interoperability Consultative Committee;

(c) any recommendations by the European Telecommunications Standards Institute; and

(d) any recommendations by the Telecommunications Standards Bureau (formerly the International Telegraph and Telephone Consultative Committee) of the International Telecommunication Union.

8.2 The Customer agrees to connect the CPE and other equipment to the Connectivity Services only by using the Network Termination Equipment provided by the Company with the Connectivity Services.

8.3 All Services Equipment remains the property of the Company at all times.

8.4 The Customer agrees:

8.4.1 to prepare the Customer Premises and provide a suitable place, conditions, connection points and electricity for the Services Equipment at the Customer Premises in accordance with the Company's reasonable instructions, if any;

8.4.2 to obtain all necessary consents, including for example, consents for any necessary alterations to buildings, permission to cross other people's land or permission to install the circuit connection and/or Services Equipment on their property; and

8.4.3 at its own cost, to return any Services Equipment within thirty (30) days (unless otherwise agreed) of request from the Company on the termination of this Contract.

8.5 During the Term, the Customer is responsible for the Services Equipment and agrees to take reasonable steps to ensure that nobody (other than someone authorised by the Company) adds to, modifies or in any way interferes with it. The Customer will be liable to the Company for any loss of or damage to the Services Equipment, except where such loss or damage is due to fair wear and tear or is caused by the Company, or anyone acting on the Company's behalf.

8.6 The Customer shall not move any Services Equipment at the Customer Premises, without the Company's prior approval (not to be unreasonably withheld or delayed).

9 POINT TO POINT LEASED LINE SERVICES

9.1 When a Point to Point Lease Line Service is specified in the Order Form, the Company will provide a Leased Line delivered 'point to point' between those Customer Premises identified in the Order Form for the Point to Point Leased Line Service.

9.2 The Point to Point Leased Line Service will also include a break-out for general access to the internet, unless otherwise agreed.

9.3 The Point to Point Leased Line Services will not share infrastructure with the Company Network and will be delivered as a standalone service that will not be monitored by the Company.

10 WAN CONNECTIVITY SERVICES

MPLS

10.1 Where stated in the Order Form that the Company is providing MPLS connectivity, it will include:

10.1.1 a core network comprised of MPLS;

10.1.2 the access option(s) stated in the Order Form: ADSL, ADSL2+, FTTC,SOADSL, SOGEA, FTTP, GEA, EoFTTC, EoFTTP, EFM or Fibre Ethernet (leased line), together with the corresponding Bandwidths and bearers for the access options(s) selected, where applicable; and

10.1.3 the additional resiliency options stated in the Order Form (if any).

10.2 Where expressly identified in the Order Form, the MPLS will in addition include:

10.2.1 internet connectivity; and

10.2.2 a centrally hosted firewall to be managed in accordance with Specific Conditions G1 – Local Area Network Services.

MPLS Access Types

10.3 **Wires Only**

10.3.1 Where stated in the Order Form that the Company is providing a Wires Only solution, the Company will provide only the circuit connection to the Customer Premises as stated in the Order Form.

10.3.2 Any routers and other CPE are to be provided, installed and maintained by the Customer.

10.3.3 The Demarcation Point at the Customer Premises for the Wires Only Connectivity Services will be the interface of the external circuit connection with the Network Termination Equipment.

10.4 **Wires and Managed Equipment**

10.4.1 Where stated in the Order Form that the Company is providing a wires and Managed Equipment solution, the Company will:

(a) provide the circuit connection to the Customer Premises as stated in the Order Form; and

(b) provide the Managed Equipment as set out in the Order Form, such Managed Equipment remaining owned by the Company, unless otherwise stated in the Order Form.

10.4.2 The Demarcation Point at the Customer Premises for wires and Managed Equipment will be the internal LAN interface port on the CPE.

SD-WAN

10.5 Where stated in the Order form that the Company is providing SD-WAN connectivity, it will include:

10.5.1 a core network comprised of SD-WAN;

10.5.2 the access option(s) stated in the Order Form: ADSL, ADSL2+, FTTC, SOADSL, SOGEA, FTTP, GEA, EoFTTC, EoFTTP, EFM or Fibre Ethernet (leased line), together with the corresponding Bandwidths and bearers for the access options(s) selected, where applicable;

10.5.3 the additional resiliency options stated in the Order Form (if any); and

10.5.4 the Managed Equipment as set out in the Order Form, such Managed Equipment remaining owned by the Company, unless otherwise stated in the Order Form.

10.6 Where expressly identified in the Order Form that the SD-WAN Connectivity Services will include a centrally hosted and/or local firewall, such firewall will be managed in accordance with Specific Conditions G1 – Local Area Network Services.

10.7 The Demarcation Point at the Customer Premises for the SD-WAN Connectivity Services will be the internal LAN interface port on the CPE.

Mobile Data Connectivity

10.8 Where stated in the Order Form that the Company is providing Mobile Connectivity Services, the terms and conditions set out in Specific Conditions M3 – Daisy Multi Network IOT Services will apply in addition to these Specific Conditions and, in the event of any conflict, the terms and conditions set out in Specific Conditions M3 – Daisy Multi Network IOT Services will take precedence over these Specific Conditions in respect of any 4G Connectivity Services.

11 MANAGED SERVICES

11.1 Where Managed Equipment for Connectivity Services is specified in the Order Form, the Company will monitor and manage such Managed Equipment and the configuration and interconnections of such Managed Equipment and in particular will:

11.1.1 continuously monitor the Managed Equipment and provide Event Management for any alerts raised by this monitoring;

11.1.2 notify the Customer of any pre-agreed Events raised by monitoring;

11.1.3 complete basic diagnosis with the aim of identifying the reason for any Event raised by monitoring and, where appropriate, take action to mitigate performance degradation or outages;

11.1.4 provide Incident Management for any Incidents raised by Event Management or by the Customer for the Managed Equipment;

11.1.5 provide Problem Management for the Managed Equipment;

11.1.6 subject to paragraph 11.1.7, update the firmware or software for the Managed Equipment identified by the Company or requested by the Customer. Any updates will be agreed with the Customer before being applied in accordance with Change Management and the Customer will not unreasonably withhold or delay agreement. Any updates or upgrades requested by the Customer as a Service Request will incur additional cost on a time and materials basis, which will be agreed with the Customer prior to such work being completed;

11.1.7 where the Managed Equipment is a cloud managed device with Vendor supported patching such as an SD-WAN appliance, schedule the Managed Equipment to auto update on a regular patch cycle within an update maintenance window as notified to the Customer from time to time. If the Customer requires the update to be deferred or rescheduled or supported outside of Normal Working Hours additional charges may apply, which the Company will notify to the Customer in advance of being incurred;

11.1.8 collate configuration backups pre- and post-implementation of a Change to the Managed Equipment and maintain at least one current configuration backup at all times and at least the two most recent previous configuration backups for one month after they are superseded by the current configuration, insofar as this can be reasonably supported by the Vendor technology and management toolset; and

11.1.9 where the Company also provides break-fix maintenance services for the Managed Equipment (as set out in the Order Form or as provided in accordance with a separate contract between the Company and the Customer), notify the Service Desk of any pre-agreed Events regarding the Managed Equipment.

12 MANAGED FORTINET SD-WAN OVERLAY

Syndicated Management Platform

12.1 Where specified in the Order Form that the Company is providing Syndicated Management Platform, the Company will:

12.1.1 provide a FortiManager segregated software environment within the Syndicated Management Platform; and

12.1.2 provide a FortiAnalyzer segregated software environment within the Syndicated Management Platform.

Dedicated Management Platform

12.2 Where specified in the Order Form that the Company is providing Dedicated Management Platform, the Company will:

12.2.1 provide a FortiManager software environment within the Dedicated Management Platform; and

12.2.2 provide a FortiAnalyzer software environment within the Dedicated Management Platform.

SD-WAN Overlay Monitoring and Event Management

12.3 Where specified in the Order Form that the Company is providing SD-WAN Overlay Monitoring and Event Management, the Company will monitor the Managed Equipment and the configuration and interconnections of such Managed Equipment and in particular will continuously monitor the Managed Equipment and provide Event Management for any alerts raised by this monitoring.

SD-WAN Overlay Reactive Technical Support

12.4 Where specified in the Order Form that the Company is providing SD-WAN Overlay Reactive Technical Support, the Company will:

12.4.1 resolve Incidents in accordance with the Incident Management process;

12.4.2 investigate Problems in accordance with the Problem Management process;

12.4.3 implement Changes in accordance with the Change Management process; and

12.4.4 maintain a configuration management database in relation to the Managed Fortinet SD-WAN Overlay and update the stored configuration items on a regular basis.

SD-WAN Overlay Security Updates

12.5 Where specified in the Order Form that the Company is providing SD-WAN Overlay Security Updates, the Company will, upon identification of a Security

Update being made available by the Vendor, update the firmware or software for the Managed Equipment identified by the Company or requested by the Customer. Any updates will be agreed with the Customer before being applied in accordance with Change Management and the Customer will not unreasonably withhold or delay agreement. Any updates or upgrades requested by the Customer as a Service Request will incur additional cost on a time and materials basis, which will be agreed with the Customer prior to such work being completed.

SD-WAN Overlay Asset Management

12.6 Where specified in the Order Form that the Company is providing SD-WAN Overlay Asset Management, the Company will provide a report with details on:

(a) licence status;
(b) location;
(c) statistics; and
(d) registration status.

SD-WAN Overlay Monthly Health Reporting

12.7 Where specified in the Order Form that the Company is providing SD-WAN Overlay Monthly Health Reporting, the Company will provide a report with details on:

(a) performance; and
(b) utilisation.

12.8 The reporting referred to in paragraph 12.7 will be generated using the native capability of the Customer's segregated software environment within the Management Platform and as such is subject to the Customer's available license and subject to change without notice.

SD-WAN Overlay Review Meeting

12.9 Where specified in the Order Form that the Company is providing SD-WAN Overlay Review Meeting, the Company will at the frequency stated in the Order Form, attend a call of no more than one (1) hours duration (unless otherwise specified in the Order Form) to review and where relevant, make recommendations, relating to the reporting referred to in paragraph 12.7.

SD-WAN Overlay IPS Reporting

12.10 Where specified in the Order Form that the Company is providing SD-WAN Overlay IPS Reporting, the Company will at the frequency stated in the Order Form, provide a report of threats detected and blocked by the IPS components of the Supported Hardware and Software.

SD-WAN Overlay Security Review Meeting

12.11

Where specified in the Order Form that the Company is providing SD-WAN Overlay Security Review Meeting, the Company will, at the frequency stated in the Order Form, attend a call of no more than one (1) hours duration (unless otherwise specified in the Order Form) to discuss the results of the report specified in paragraph 12.9 and agree if any updates are required. Following such call, the Company will carry out any agreed updates to the configuration of the IPS of the Managed Equipment.

Co-Management Services

12.12 Where specified in the Order Form that the Company is providing Co-Management Services, the Company will provide the Customer with access to the Management Platform to allow the Customer to make configuration changes. The Customer acknowledges and agrees that:

12.12.1 access to the Management Platform will be granted in the form of named individual login credentials. All login credentials must be provided by the Company and must not be copied or distributed by the Customer;

12.12.2 on request by the Company, Customer administrators must provide evidence of appropriate Vendor training (including in relation to secure firewall policies);

12.12.3 it shall notify the Company where Customer administrators no longer require access to the Management Platform;

12.12.4 it will at all times comply with all Relevant Laws including but not limited to the Telecommunications (Security) Act 2021;

12.12.5 it will at all times comply with the Statement of Works;

12.12.6 it will maintain a Change Management policy and all configuration changes will comply with such policy;

12.12.7 it will notify the Company prior to any configuration changes being performed;

12.12.8 the Company will not be liable to the Customer for any loss or other impact suffered by the Customer as a result of any configuration changes made by the Customer or anyone acting on the Customer's behalf;

12.12.9 notwithstanding clause 12.12.8, if the Customer or anyone acting on the Customer's behalf, makes any configuration changes which impact the Connectivity Services, as demonstrated by the Management Platform, any Enhanced Service Levels will not apply and the Company may carry out remedial work to rectify such impact, such work being chargeable by the Company on a time and materials basis; and

12.12.10 it will indemnify and keep indemnified the Company against all liabilities, losses, actions, proceedings, damages, costs (including legal costs), claims, demands and expenses brought or made against or suffered or incurred by the Company or any of its customers or suppliers arising out of or connected with any configuration changes made by the Customer or anyone acting on the Customer's behalf.

13 CLOUD CONNECTIVITY SERVICES

13.1 Where stated in the Order form that the Company is providing Cloud Connectivity Services, it will provide a private direct connection either from the Customer's WAN or from the Customer's Premises as set out in the Order Form to the Customer's cloud service provider (e.g. Amazon Web Services (AWS) or Microsoft Azure) as stated in the Order Form that will include:

13.1.1 the access option(s) stated in the Order Form together with the corresponding Bandwidths;

13.1.2 the additional resiliency options stated in the Order Form (if any);

13.1.3 the port connection options into the Customer's cloud service provider; and

13.1.4 the Managed Equipment (if any) as set out in the Order Form, such Managed Equipment remaining owned by the Company, unless otherwise stated in the Order Form.

14 DDP SERVICES

14.1 Where stated in the Order Form that DDP Services are being provided, the Company will:

14.1.1 work with the Customer to configure a policy specific to the Customer to attempt to automatically detect a suspected DDoS Attack and re-route the Customer's traffic to the Company's mitigation infrastructure;

14.1.2 during a suspected DDoS Attack, use reasonable endeavours to automatically re-route the Customer's traffic to the mitigation infrastructure; filter legitimate traffic from DDoS Attack traffic and forward what is believed to be legitimate traffic, whilst suspected DDoS Attack traffic is discarded by the mitigation infrastructure;

14.1.3 monitor any alerts generated by the Managed Equipment regarding any potential or suspected DDoS Attack that indicate a suspected DDoS Attack but have not triggered automatic re-routing and notify the Customer of any such alerts and manage such alerts in accordance with paragraph 14.1.4 and in accordance with the Company's Incident Management process; [to be stated on the order form IP address ranges to be protected, bandwidth protected (mbps)]

14.1.4 during a suspected DDoS Attack where automatic re-routing has not occurred and, following notification by the Company to the Customer in accordance with paragraph 14.1.3, where it is agreed between the Company and the Customer that a DDoS Attack is taking place, use reasonable endeavours to manually re-route the Customer's traffic to the Company's mitigation infrastructure;

14.1.5 where re-routing has occurred, and the Customer believes that either legitimate traffic is being discarded or DDoS Attack traffic is being forwarded, use reasonable endeavours to investigate and reconfigure the policy to address this in accordance with the Company's Incident Management process;

14.1.6 provide a mitigation report following the occurrence of a suspected DDoS Attack within 5 (five) Business Days, stating the attack size and mitigation measures implemented by the DDP Services; and

14.1.7 provide Problem Management for the DDP Services.

14.2 The Company makes no representation that the DDP Services will withstand or mitigate the effects of any or all DDoS Attack traffic, will not block or affect any legitimate traffic, or will prevent denial of access to any service of the Customer.

14.3 Unless expressly stated otherwise in the Order Form, the provision of DDP Services is dependent on the Company providing the connections over which the Customer's legitimate traffic is normally routed to the Customer as part of the Connectivity Services pursuant to this Contract. If for any reason the Company ceases to provide the relevant Connectivity Services to the Customer, the DDP Services shall terminate with immediate effect and without liability for the Company.

15 GENERAL

15.1 The Company will:

15.1.1 implement capacity planning and be responsible for the network infrastructure in respect of the Company Network used to deliver Internet Access;

15.1.2 configure and provide IP network ranges in accordance with the regulations of Reseaux IP Europeens (RIPE) and RFC1918 (if applicable);

15.1.3 communicate any planned works notifications;

15.1.4 investigate any unplanned service outages with the Service Provider; and

15.1.5 communicate Reason for Outage Reports (RFO) where applicable.

15.2 The Company may suspend any or all of the Connectivity Services, or performance of any or all of its obligations under this Contract, in the following circumstances without liability at any time:

15.2.1 during any technical failure, modification, repair, testing or maintenance of the Network or other equipment by which the Connectivity Service is provided, or in the case of emergency; and/or

15.2.2 if the operation of the Network or the provision of the underlying services to the Company is suspended for any reason.

15.3 Without prejudice to any of the Company's other rights and remedies, the Company may on notice to the Customer disconnect any or all of the Connectivity Services or suspend performance of any or all of its obligations under, or terminate, this Contract in the following circumstances without liability if:

15.3.1 any licence or permission to operate or use the Network or any part of it is revoked or terminated for any reason;

15.3.2 the operation of the Network is terminated or if the provision of the underlying service to the Company is discontinued for any reason;

15.3.3 the Customer does or allows to be done anything that in the Company's reasonable opinion will or might jeopardise the operation of the Connectivity Services or the Network; or

15.3.4 the Company reasonably suspects the Connectivity Services are being used in a manner prejudicial to the interests of the Customer or the Company.

15.4 Where the Company determines, using its sole discretion, that the Customer is under a DDoS Attack that directly or indirectly threatens the Connectivity Services or the integrity of the Company Network and its ability to provide services to its other customers:

15.4.1 the Company reserves the right to divert and discard all of the Customer's traffic (legitimate or otherwise);

15.4.2 the Customer acknowledges that it may irretrievably lose such traffic and associated data and the Company shall not be held responsible for such loss of traffic, legitimate or otherwise; and

15.4.3 the Customer acknowledges that this action may be taken irrespective of whether DDP Services are being provided.

15.5 Where the Company agrees to supply any IP Addresses, as expressly provided in the Order Form:

15.5.1 any such IP Address that may be supplied by the Company to the Customer is licensed to the Customer on a non-exclusive, non-transferable, revocable basis for use only in conjunction with the relevant Services Equipment and the Connectivity Services and will remain the Company's property;

15.5.2 following disconnection of the Connectivity Services the Customer's licence to use any IP Address supplied by the Company will automatically terminate; the Customer will not make any further use of it (unless otherwise agreed in writing); and it may be re-assigned by the Company either to the Company itself or to a third party; and

15.5.3 the Company reserves the right to charge the Customer for any IP Address used or retained by the Customer after termination of this Contract.

16 CUSTOMER OBLIGATIONS

16.1 The Customer shall:

16.1.1 where the Managed Equipment is located on Customer Premises:

(a) provide reasonable on-site 'remote hands' assistance, such as power cycling the Managed Equipment, to troubleshoot and diagnose any issues;

(b) ensure that all Managed Equipment is housed in an appropriately secure, well-ventilated cabinet with sufficient environmental control to maintain both heat and moisture within tolerable limits; and

(c) ensure the power supply to the Managed Equipment is protected to maintain continuous supply and prevent spikes and losses;

16.1.2 not configure, maintain or modify (or permit any third party to do so) any Managed Equipment without the prior written consent of the Company;

16.1.3 be responsible for any third party services or infrastructure that it provides to enable the provision of the Connectivity Services;

16.1.4 maintain subscriptions to Vendor-specific software assurance programs for the duration of this Contract in respect of the Managed Equipment;

16.1.5 ensure that Company is named as an authorised representative of the Customer where required on any third party break-fix maintenance agreements;

16.1.6 notify the Company of any contact details or address changes of the Customer;

16.1.7 unless otherwise expressly provided in the Order Form, define all IP Addresses relevant to the Connectivity Services;

16.1.8 in respect of any SD-WAN Services that connect over any part of a Network that is not part of the Company Network allocate the IP Address block(s) for the Company;

16.1.9 ensure that the Company is named as an authorised representative of the Customer where required, on any third-party break fix maintenance agreements relevant to the Third Party Break-Fix Maintenance;

16.1.10 in respect of any DDP Services:

(a) maintain a relevant internal emergency/incident response procedure for dealing with DDoS Attacks;

(b) provide the Company with an up-to-date point of contact with 24x7 availability who the Company shall coordinate with upon the detection of a DDoS Attack;

(c) inform the Company promptly of any changes made to its hardware or software IT infrastructure (including but not limited to any changes to its network, systems or policy) that may affect the DDP Services; and

(d) ensure that suitable Customer Representatives are available to discharge the Customer's responsibilities in connection with the DDP Services, including but not limited to replying to and executing such steps as are reasonably necessary to address a fault or a DDoS Attack and providing the Company with relevant information and decisions in a timely manner, as reasonably requested by the Company during a DDoS Attack; and

16.1.11 not use or facilitate the use of the Connectivity Services to (including by pointing to websites or locations that) create, transmit, distribute or store materials that include tools designed for compromising security (including but not limited to password guessing programs, cracking tools or network probing tools) data protection or anti-terrorism laws, impair the privacy of communication or knowingly contain Viruses or otherwise knowingly and/or intentionally transmit, introduce or allow a Virus to be introduced through the Connectivity Services.

16.2 The Customer Obligations set out in paragraph 16.1 apply to the Connectivity Services, and Company shall have no liability for any failure to provide the Connectivity Services (including failing to meet any Service Level), or to pay any Service Credit (if applicable), to the extent caused by any failure by the Customer to provide any secure connectivity from the Company's management systems to the Managed Equipment that is required to enable remote configuration or management of the Managed Equipment by the Company.

17 EXCLUSIONS

17.1 In providing Connectivity Services, unless otherwise expressly stated to the contrary in this Contract, the Company is not providing:

17.1.1 any security services and therefore will not be liable for any security-related attacks or impact that causes any loss to the Customer, save as otherwise expressly provided in the Order Form or this Contract;

17.1.2 any software licence renewals or security certificate renewals; or

17.1.3 any hardware, licensing and/or security certificates that are required to meet the pre-requisites for any code upgrades released by the Vendor.

17.2 In respect of the DDP Services, unless otherwise expressly stated to the contrary in the Contract, the Company makes no representation that the DDP Services will be error-free, will withstand or mitigate the effects of any or all DDoS Attack traffic, will not block or affect any legitimate traffic, or will deny access to any service of the Customer.

18 CHARGES

18.1 The Charges for the Connectivity Services are as identified in the Order Form.

18.2 The Charges for the Connectivity Services will apply from the relevant Connection Date for the relevant Connectivity Services.

18.3 The Company shall have the right to alter the Charges for the Connectivity Services from time to time to account for any price changes imposed by Carriers or Service Providers.

18.4 Usage charges payable shall be calculated by reference to data recorded or logged by the Company and not by reference to any data recorded or logged by the Customer. Any invoices issued by the Company in respect of the Charges for Connectivity Services shall, save in the case of manifest error, be final, conclusive and binding on the Customer.

19 INVOICING AND PAYMENT

19.1 Subject to paragraph 19.2, the Customer will be invoiced monthly in arrears by the Company for any volume based usage of the Services.

19.2 Charges shall be payable monthly in advance, unless expressly agreed in writing by the Company and set out in the Order Form.

20 SERVICE LEVELS

20.1 **Incident Management**

The Company will provide Incident Management for Connectivity Services in accordance with the Service Levels set out in Specific Conditions X3 – Standard Operational Services.

20.2 **Broadband Services Target Resolution Times for Faults**

20.2.1 Incident resolution for Broadband Services will be provided by the relevant Carrier during the hours of support set out at Table 1 below. The Incident classification matrix set out below outlines the description, resolution and scheduled updates frequencies for the associated Incident priorities for Broadband Services only, as provided by the relevant Carrier.

Table 1: Broadband Services - Carrier Target Resolution Times by Priority Level

		Carrier			
Care Level	**Hours of Support**	**BT Wholesale**	**TalkTalk Business**	**Exclusions**	**Requirement**
Standard Care	Normal Working Hours	40 WH	48 WH	Regional public and bank holidays. Allowable parked times	Included
Enhanced Care	24 x 7	20 CH	24 CH	Allowable Parked Time	Optional
Premium Care	24 x 7	7 CH	N/A	Allowable Parked Time	Optional

CH = Clock Hour (i.e. regular full day round-the-clock hours)
WH = Normal Working Hours

20.2.2 **Standard Care:** To the extent this level of care is stated in the Order Form, the Company will use its reasonable endeavours to procure that the Carrier acknowledges the fault upon receipt and clears the fault within the time set out in Table 1 above. Engineer appointments to Customer Premises are available 0800-1800 Monday to Saturday (excluding Regional Public and Bank Holidays).

20.2.3 **Enhanced Care:** To the extent this level of care is stated in the Order Form, the Company will use its reasonable endeavours to procure that the Carrier acknowledges the fault upon receipt and clears the fault within the time specified in Table 1 above. Engineer appointments to site are available 0800-1800 Monday to Sunday (including Regional Public and Bank Holidays). Out of hours engineering visits to the Customer Premises may be used at the Carrier's discretion to complete a repair if unrestricted access is available.

20.2.4 **Premium Care:** To the extent this level of care is stated in the Order Form, the Company will use its reasonable endeavours to procure that the Carrier acknowledges the fault upon receipt and clears the fault within the time specified in Table 1 above. If diagnostics indicate a fault and an engineer is required on site, then the Carrier will aim to fix any fault within 7 (seven) hours from the start time of the agreed appointment slot, excluding any Allowable Parked Time. Out of hours engineering visits to site may be used at the Carrier's discretion to complete a repair if unrestricted access is available.

21 MANAGED INTERNET ACCESS AND WAN SERVICES TARGET RESOLUTION FOR FAULTS

21.1 The Incident classification matrices set out in Table 2 and 3 below outline the description and target resolution times for the associated Incident priorities.

Table 2:

	Priority Level	**Target Resolution Time**
P1	Critical	4 hours
P2	High	8 hours
P3	Normal	48 hours
P4	Minor	4 Business Days

Table 3:

Priority Level		**Examples**
P1	Critical Incident	Significant revenue, operational or safety impact on the Customer. A total loss of Service affecting a single Customer Premises or multiple departments or business functions of the Customer. A Service is significantly degraded affecting the entire Customer organisation.
P2	High Risk Incident	A total loss of a Service affecting a single department or business function of the Customer. A Service is degraded or impacted affecting multiple departments or a single Customer Premises.
P3	Medium Risk Incident	A Service is degraded or impacted affecting a single department or business function of the Customer. A Service is degraded or a total loss of Service for an individual End User.
P4	Minor Incident	Any incident not classified as a P3 or above.

21.2 Where the fault lies with the Service Provider, the Company shall use its reasonable endeavours to procure that the Service Provider acknowledges and clears the fault within the target resolution time set out in Table 2 above, excluding any Allowable Parked Time. However, the Service Provider's target resolution times will prevail and the Company's target resolution times will be placed on hold for any third party fix.

21.3 Where the fault is found to lie with the CPE the Company will use its reasonable endeavours to replace the CPE on the next business day or in line with the supplied breakfix service level agreement.

22 AVAILABILITY SLA

22.1 The Company will assign an availability category ("Site Category") to each Customer Premises determined by the Service and configuration.

22.2 The Site Category will, if applicable, be specified on the Order Form. Where no Site Category is specified on the Order Form, no service level agreement applies in respect of that Service.

22.3 The target minimum Service Availability is as set out in Table 4 below. Service Availability is calculated in accordance with paragraph 24.1. The target minimum Service Availability depends on the access options and/or resiliency options chosen by the Customer.

Table 4:

Type	Site Category	Target Service Availability (Mthly)
Resilient	Cat A+	99.999%
	Cat A	99.995%
	Cat B	99.99%
	Cat C	99.95%
Standard	Cat D	99.93%
	Cat E	99.85%
	Cat F	99.80%
	Cat G	97.00%
Non Standard	NS	As per Order Form

22.4 Service Availability for Managed Internet Access, Broadband and WAN access circuits is measured on the Uptime of the Customer Premises, based on the availability of the circuit(s) terminating into the CPE at the Customer Site.

22.5 Service Availability for Cloud Connectivity is measured from the interface on the Company's routers or CPE to the interface at the cloud service provider PoP.

23 WAN NETWORK PERFORMANCE

23.1 Network performance service levels apply to the Company on network traffic. The standard network performance service levels measures performance on the Company network and does not include the Customer's access to the Company network.

23.2 Network performance applies to traffic within the UK only for WAN networks connected to the Company UK PoPs.

23.3 The specific targets for network performance are as set out below, unless otherwise specified in the Order Form:

	Target		
Performance Type	**BE Class**	**AF Class**	**EF Class**
Latency (in ms)	30	20	15
Packet Loss (%)	0.3	0.1	0.05
Jitter (in ms)	N/A	N/A	2.0

23.4 The Company network performance metrics are collected through specific tests which are each conducted at 1400 byte packets set at three second intervals 15 times every 60 seconds.

23.5 For the avoidance of doubt, planned maintenance and emergency maintenance are excluded from the calculation of the performance targets in accordance with paragraph 25.

24 AVAILABILITY

24.1 **Availability Calculation**

The Service Availability of the Connectivity Services is defined and calculated separately for each Customer Premises. Subject to paragraph 24.3, the Service Availability of the Connectivity Services is measured as a percentage and is a representation of the portion of time that the relevant service is available during the Measurement Period calculated in accordance with this paragraph 24,1. The Connectivity Services are deemed available if data packets can be transmitted over the Connectivity Service from the Demarcation Point to the first PoP in the Company Network and such transmission is within the parameters of the relevant Service Levels for Packet Loss and/or Latency.

Availability is calculated using the following formula:

$$Availability = \frac{(AST-DT)}{AST} x\ 100$$

Where:

AST = Agreed Service Time (which unless otherwise agreed is the total number of minutes in the Measurement Period)

DT = Downtime being the actual time that the Connectivity Services are Unavailable during the Agreed Service Time

24.2 **Service Measurement Period**

Unless otherwise agreed in the Order Form, the Company's performance against the Service Levels will be measured each calendar month on the first day of the calendar month following the Connection Date (the "**Measurement Period**"). Save in the case of manifest and demonstrable error, the Company's performance against the Service Levels shall be based solely on information recorded by the Company.

24.3 **Service Level Exclusions and Exemptions**

24.3.1 Any downtime or unavailability of the Connectivity Services to the extent caused by the following, will not be classified as Unavailable for the purposes of the calculation of the Availability in accordance with these Specific Conditions and the following shall not be taken into account for the purposes of any other Service Level calculations and such matters shall not be counted or considered in relation to any performance by the Company of any Service Level or other term or condition of this Contract:

(a) the Customer's network, system or equipment, or any part of it (including without limit Customer Provided Apparatus) or any other network or equipment outside of the Company Network;

(b) the Customer's and/or its agents', representatives' and users' negligent acts or omissions;

(c) the Customer's breach of this Contract or any negligent, wilful or reckless act, fault or omission by the Customer, or any users of the Connectivity Services for whom the Customer is responsible;

(d) the failure of the Customer to agree to the application of required software patches;

(e) the Customer's failure or delay in complying with the Company's reasonable instructions and/or any failure or delay in providing information requested by the Company;

(f) any delay in the Customer allowing the Company and/or the Company Personnel, to enter into a Customer Premises and/or the applicable parts thereof to diagnose or remedy any fault; or

(g) anything beyond the reasonable control of the Company including without limitation in respect of the failure of any Carrier or Service Provider to provide network capacity or connectivity (or any element thereof) to the Company on which it was reliant for the purposes of the Contract, any Act Of God, terrorist attacks, severe weather, accidental damage, vandalism, failure or shortage or power supplies (other than those for which the Company is responsible under this Contract), flood, drought, lightning or fire, any act or omission of Government, highways authorities, or other competent authorities;

(h) any Customer encryption on any of the routers preventing Company access;

(i) the Customer requesting the Company to modify Managed Equipment or any other part of the Customer's network at a Customer Premises, or test it although no fault has otherwise been detected or reported in accordance with the terms of this Contract;

(j) implementation of a configuration Change in accordance with the Customer's instructions;

(k) subject to paragraph 25, Planned Outages or emergency maintenance;

(l) maintenance carried out by the Customer or the Company on the Customer's instructions;

(m) power outages at a Customer's Premises;

(n) relocation, reconfiguration, modification and/or reprogramming of Managed Equipment, Customer Equipment that is not undertaken by the Supplier unless completed under (and strictly in accordance with) the Supplier's instructions;

(o) suspension of the Connectivity Services in accordance with this Contract;

(p) environmental conditions at a Customer's Premises that are not within the tolerances prescribed by the relevant manufacturer's guidelines (for example humidity, heat, dust, power);

(q) any fault in a circuit between the local exchange and the applicable Customer Premises where the Connectivity Services at a Customer Premises includes circuits from dual carriers (using the same duct) and does not have the benefit of full fibre diversity into the Customer Premises from a single Carrier);

(r) where resiliency options are provided in the Order Form (if any), the network convergence (failover) time will not be considered as Unavailability;

(s) an abnormally-high Latency and/or Packet Loss measurement, due to the Connectivity Services being congested because of the acts or omissions of the Customer;

(t) where the Connectivity Services are Wires Only and the Customer has not provided suitable CPE and/or configuration to take advantage of a backup circuit that forms part of the service availability (for example a backup EFM circuit); or

(u) any act or omission of any third party that is beyond the Company's reasonable control, which includes, without limitation, fibre cutting.

24.3.2 The Supplier's monitoring tools may show access mechanisms as "up" (available) or "down" (unavailable). This must not be confused with the availability of the Connectivity Services for the purposes of the Service Levels.

24.3.3 In respect of any xDSL Connectivity Services:

(a) the Company does not guarantee local loop line quality and therefore cannot guarantee that all lines can support the prioritised Upstream and minimum Downstream data rates specified for Connectivity Services where stated;

(b) the achievable Bandwidth and data rates of any xDSL Connectivity Services are subject to the quality of the copper and distance from the Network exchange; and

(c) some limitations within the local loop Network may not become apparent through no fault of the Company until after an xDSL Connectivity Service has been installed and working for some time, for example copper quality degradation.

25 PLANNED AND EMERGENCY MAINTENANCE

25.1 From time to time the Company may interrupt the Service to maintain, update or enhance software, equipment or other aspects of the Service and/or the Company Network. The Company will, where possible, give the Customer a minimum of 5 Business Days' advance notice of such events, and where possible will schedule maintenance events so as to cause minimum interruption of the Service.

25.2 The Company will use its reasonable endeavours to ensure that:

25.2.1 scheduled maintenance events will not exceed 3 hours in any calendar month; and

25.2.2 emergency maintenance events will not exceed 3 hours in any calendar month.

25.3 The Customer accepts that it may not be possible for the Company to provide the Customer with advanced notification of emergency maintenance events.

26 SERVICE CREDITS

26.1 The Company will use its reasonable endeavours to recover service credits from the Carrier and/or the Service Provider (where such credits are contractually payable to the Company) and if service credits are received from the Carrier and/or the Service Provider, these will be passed on to the Customer.