

SPECIFIC CONDITIONS G1 – LOCAL AREA NETWORK SERVICES

These Specific Conditions govern the Local Area Network 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, which shall be deemed to be incorporated into the Contract for the performance of any Local Area Network Services performed under these Specific Conditions.

The Local Area Network Services set out under the headings "Deliverables", "WiFi Engage Services", "WiFi Protect Services" and "Friendly WiFi" will be provided by the Company only if 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:

"Advanced WiFi Monitoring"	means the Services provided by the Company in accordance with paragraph 5.7;
"Device Patching"	means the Services provided by the Company in accordance with paragraph 5.2;
"Enterprise"	means a Service Option in relation to the Local Area Network Services provided by the Company in accordance with paragraph 4.2;
"Enterprise Plus"	means a Service Option in relation the Local Area Network Services provide by the Company in accordance with paragraph 4.3;
"Essentials"	means a Service Option in relation the Local Area Network Services provide by the Company in accordance with paragraph 4.1;
"Fair Usage Policy"	means the policy for the reasonable and fair use of the Local Area Network Services as set out in paragraph 13;
"FortiAnalyzer"	means software provided by Fortinet Inc, working with FortiManager, for storing data intended for analysis;
"FortiManager"	means software provided by Fortinet Inc for managing devices;
"Friendly WiFi"	means the Services to be provided by the Company to the Customer in accordance with paragraph 8;
"Health Check"	means the Services provided by the Company in accordance with paragraph 5.3;
"IPS Policy Management"	means the Services provided by the Company in accordance with paragraph 5.6;
"Licence"	means the licence granted by the Company to the Customer to use the WiFi Engage Software in accordance with the terms of these Specific Conditions;
"Local Area Network Services"	means the Services to be provided by the Company to the Customer in accordance with these Specific Conditions as specified in an Order Form;
"Maintenance Services"	means a form of break-fix maintenance service which is provided by the Company or by a third party;
"Operational Event Monitoring"	means the Services provided by the Company in accordance with paragraph 5.1;
"Palo Alto Networks Panorama"	means the firewall management platform designed and licensed by the Palo Alto Networks company for the purposes of managing firewalls manufactured by the Palo Alto Networks company;
"Remote Security Advice"	means the Services provided by the Company in accordance with paragraph 5.5;
"Remote Technical Advice"	means the Services provided by the Company in accordance with paragraph 5.4;
"Service Option"	means Enterprise, Enterprise Plus or Essentials as set out in the Order Form;
"Shared Panorama"	means the Services provided by the Company in accordance with paragraph 5.8;
"Software Documentation"	means any documentation, user manuals or other information made available by the Company to the Customer to aid in the operation and use of the WiFi Engage Software;
"Supported Hardware and Software"	means the equipment and software specified as such in the Order Form in respect of which the Company will provide the Local Area Network Services, as specified in the Order Form, including but not limited to routers, network switches, wireless local area network controllers, wireless access points, firewalls and load balances;
"Syndicated Management Platform"	means a software build of the Fortinet Inc management platform within the Company's shared infrastructure;
"WiFi Engage Services"	means the WiFi Engage Software and connected services provided by the Company in accordance with paragraphs 6 and 7;
"WiFi Engage Software"	means the software provided to the Customer by the Company in connection with the WiFi Engage Services, which is owned by or licensed to the Company and purchased by the Customer in the volumes set out in the Order Form; and
"WiFi Protect Services"	means a cloud-delivered security service, which uses Third Party Software, provided and managed by the Company in accordance with paragraph 14, that provides content filtering for the Customer and/or its End User when accessing the internet from the Customer's wireless access points.

1.2 All other capitalised terms that are not defined in paragraph 1.1 shall have the meanings stated in the Conditions and/or Specific Conditions X3 – Standard Operational Services.

2 COMMENCEMENT DATE

2.1 The Commencement Date of the Local Area Network Services shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of the Local Area Network Services to the Customer.

3 MINIMUM TERM

3.1 The Minimum Term for the Local Area Network Services is as set out in the Order Form, or if no Minimum Term is specified, twelve (12) calendar months from the Commencement Date of the Local Area Network Services.

4 SERVICE OPTIONS

4.1 Essentials

Where specified in the Order Form that the applicable Service Option is Essentials, the Company will:

4.1.1 provide access to the Service Desk to act as a point of contact for handling Service Requests and Incidents in respect of the Supported Hardware and Software;

- 4.1.2 provide Remote Technical Advice relating to the Supported Hardware and Software;
- 4.1.3 where specified in the Order Form, provide Remote Security Advice in relation to the Supported Hardware and Software; and/or
- 4.1.4 where specified in the Order Form, provide a Health Check of the Supported Hardware and Software, at the frequency set out in the Order Form or annually if not otherwise stated.

4.2 Enterprise

Where specified in the Order Form that the applicable Service Option is Enterprise, the Company will:

- 4.2.1 provide access to the Service Desk to act as a point of contact for handling Service Requests and Incidents in respect of the Supported Hardware and Software;
- 4.2.2 provide Remote Technical Advice in relation to the Supported Hardware and Software;
- 4.2.3 provide Operational Event Monitoring of the Supported Hardware and Software;
- 4.2.4 provide Event Management for Events raised by Operational Event Monitoring;
- 4.2.5 where specified in the Order Form, provide Remote Security Advice in relation to the Supported Hardware and Software;
- 4.2.6 where specified in the Order Form, provide a Health Check of the Supported Hardware and Software, at the frequency set out in the Order Form or annually if not otherwise stated; and/or
- 4.2.7 where specified in the Order Form, provide Advanced WiFi Monitoring of the Supported Hardware and Software.

4.3 Enterprise Plus

Where specified in the Order Form that the applicable Service Option is Enterprise Plus, the Company will:

- 4.3.1 provide access to the Service Desk to act as a point of contact for handling Service Requests and Incidents in respect of the Supported Hardware and Software;
- 4.3.2 provide Operational Event Monitoring of the Supported Hardware and Software;
- 4.3.3 provide Event Management for Events raised by Operational Event Monitoring;
- 4.3.4 provide Incident Management for any Incidents relating to the Supported Hardware and Software;
- 4.3.5 provide Problem Management for any Problems relating to the Supported Hardware and Software;
- 4.3.6 complete change requests relating to the configuration of the Supported Hardware and Software, following the Service Request and Change Management processes;
- 4.3.7 complete Device Patching of the Supported Hardware and Software;
- 4.3.8 where specified in the Order Form, provide a Health Check of the Supported Hardware and Software at the frequency set out in the Order Form or annually if not otherwise stated;
- 4.3.9 where specified in the Order Form, provide Advanced WiFi Monitoring of the Supported Hardware and Software; and
- 4.3.10 where specified in the Order Form, provide IPS Policy Management on a subset of the Supported Hardware and Software as specified in the Order Form.

5 DELIVERABLES

5.1 Operational Event Monitoring

Where specified in the Order Form that the Company is providing Operational Event Monitoring, the Company will:

- 5.1.1 monitor the Supported Hardware and Software and notify the Customer by email of alerts raised by the Operational Event Monitoring; and
- 5.1.2 where specified in the Order Form that the Company is providing Operational Event Monitoring and the applicable Service Option is Enterprise Plus and:
 - (a) where the Customer has purchased Maintenance Services from the Company, the Company will instigate the hardware replacement process with the relevant third party; or
 - (b) where the Customer has purchased Maintenance Services from a third party, the Company will notify the Customer of the hardware replacement requirement and it will be the Customer's responsibility to liaise with the relevant third party to arrange hardware replacement.

5.2 Device Patching

Where specified in the Order Form that the Company is providing Device Patching, the Company will:

- 5.2.1 review firmware and software versions for Supported Hardware and Software annually to identify requirements for maintaining Vendor support and provide a report to the Customer;
- 5.2.2 review security vulnerabilities published by the Vendor to identify potentially vulnerable Supported Hardware and Software; and/or
- 5.2.3 update the firmware or software for the Supported Hardware and Software where provided by the Vendor:
 - (a) to mitigate identified security vulnerabilities;
 - (b) to mitigate stability issues or performance/functionality bugs; and
 - (c) for feature upgrades required by the Company.

5.3 Health Check

Where specified in the Order Form that the Company is providing a Health Check, the Company will:

- 5.3.1 review the existing configuration for any Supported Hardware and Software;
- 5.3.2 report to the Customer any changes that the Company recommends for consideration by the Customer to increase the performance, stability or security posture of the Supported Hardware and Software. The implementation of any such recommendations may be subject to additional Charges, as notified by the Company to the Customer. There shall be no obligation on the Company to implement any such recommended changes until any additional Charges are paid by the Customer; and
- 5.3.3 provide the Health Check as requested by the Customer, at the frequency stated in the Order Form.

5.4 Remote Technical Advice

Where specified in the Order Form that the Company is providing Remote Technical Advice:

- 5.4.1 the Company will provide a reactive technical advice line to support the Customer with responding to queries and/or resolving Incidents in respect of the Supported Hardware and Software;
- 5.4.2 the quantity of hours per month that the Company will provide Remote Technical Advice will be specified in the Order Form and will be subject to the Fair Usage Policy;
- 5.4.3 the Customer may notify the Service Desk of a question or Incident relating to the Supported Hardware and Software via telephone and/or a web portal, as directed by the Company from time to time. All Critical Incidents must be logged by the Customer via telephone with the Service Desk;

- 5.4.4 once the Customer has raised a request for Remote Technical Advice, the Company will:
- (a) create a record of the Incident and provide a reference number to the Customer;
 - (b) categorise the Incident in accordance with the priorities in paragraph 5.1 of the Specific Conditions X3 – Standard Operational Services;
 - (c) attempt to diagnose the Incident initially by telephone to ensure that a suitably qualified engineer responds to the Incident; and
 - (d) arrange for an appropriately skilled support engineer to call the Customer back within the Incident Response Time;
- 5.4.5 the Company will provide assistance via telephone or, where made available by the Customer to the Company, remotely via remote access facilities to the Customer's infrastructure; and
- 5.4.6 if it is specified in the Order Form that Remote Technical Advice is available "Out of Hours", the Company will make Remote Technical Advice available at any time; otherwise Remote Technical Advice will be available during Normal Working Hours only.

5.5 Remote Security Advice

Where specified in the Order Form that the Company is providing Remote Security Advice:

- 5.5.1 the Company will provide a reactive security advice line to support the Customer with responding to queries and/or resolving Incidents in respect of the Supported Hardware and Software;
- 5.5.2 the quantity of hours per month that the Company will provide Remote Security Advice will be specified in the Order Form and will be subject to the Fair Usage Policy;
- 5.5.3 the Customer may notify the Service Desk of a question relating to the Supported Hardware and Software via telephone and/or a web portal, as directed by the Company from time to time;
- 5.5.4 once the Customer has raised a request for Remote Security Advice, the Company will:
- (a) create a record of the request and provide a reference number to the Customer; and
 - (b) arrange for an appropriately skilled security engineer to call the Customer back and provide assistance with regard to the security events and alerts generated by the Supported Hardware and Software;
- 5.5.5 the Company will provide assistance via telephone or, where made available by the Customer to the Company, remotely via remote access facilities to the Customer's infrastructure; and
- 5.5.6 Remote Security Advice shall be available to the Customer during Normal Working Hours only.

5.6 IPS Policy Management

Where specified in the Order Form that the Company is providing IPS Policy Management, the Company will:

- 5.6.1 provide a report of threats detected and blocked by the intrusion prevention system components of the Supported Hardware and Software on a monthly basis; and
- 5.6.2 attend a call with the Customer at the frequency set out in the Order Form or quarterly if not otherwise stated, to discuss the results of the report specified in paragraph 5.6.1 and agree if any further tuning is required. Following such call, the Company will carry out any agreed updates to the configuration of the intrusion prevention system of the Supported Hardware and Software.

5.7 Advanced WiFi Monitoring

Where specified in the Order Form that the Company is providing Advanced WiFi Monitoring, the Company will:

- 5.7.1 provide a report of the performance of the WiFi network on a monthly basis; and
- 5.7.2 attend a call with the Customer at the frequency set out in the Order Form or quarterly if not otherwise stated, to discuss the results of the report specified in paragraph 5.7.1 and agree if any further tuning is required. Following such call, the Company will carry out any agreed updates to the configuration of the WiFi network.

5.8 Shared Panorama

Where specified in the Order Form that the Company is providing Shared Panorama, the Company will:

- 5.8.1 utilise the Company's multi-tenanted Palo Alto Networks Panorama management platform to collect and store logs from the Customer's firewall devices as specified in the Order Form; and
- 5.8.2 provide storage for the logs specified in paragraph 5.8.1 for a minimum of 30 (thirty) days and up to a maximum capacity, as specified in the Order Form

5.9 Syndicated Management Platform

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

- 5.9.1 utilise a FortiManager segregated software environment within the Syndicated Management Platform; and
- 5.9.2 provide storage via the FortiAnalyzer for the logs specified in paragraph 5.8.1 for a minimum of 30 (thirty) days and up to a maximum capacity, as specified in the Order Form

6 WiFi ENGAGE SERVICES

- 6.1 Where specified in the Order Form that the Company is providing the WiFi Engage Services, the Company will provide the WiFi Engage Services and the WiFi Engage Software in accordance with the terms and conditions detailed in paragraphs 6 and 7.

WiFi Engage Functionality

- 6.2 The WiFi Engage Services provides a registration and welcome back mechanism for End Users.
- 6.3 The Company will, subject to the terms of paragraphs 6 and 7, supply the Customer with the WiFi Engage Software that shall only be licensed to the Customer for use with the quantity of access points as identified in the Order Form, which are installed at the Customer Premises.
- 6.4 End Users of the WiFi Engage Services will be presented with an initial registration (landing) page that captures the End User's information including first name, surname and email address. Upon completion of the initial registration (landing) page the End User will be able to access the open internet or will have restricted access to the internet and will be redirected to specific websites as determined by the Customer's own policy.
- 6.5 The WiFi Engage Services includes a "front end captive portal" and "back end editing and reporting capability".
- 6.6 The front end captive portal includes the following features:
- 6.6.1 End User registration page presented on initial connection by the End User;
 - 6.6.2 collection of data from the End User upon initial connection of the WiFi;
 - 6.6.3 a "Thanks for registering" page presented to the End User following registration;
 - 6.6.4 automatic recognition of an End User upon a returning End User device connecting to the WiFi;
 - 6.6.5 a "Welcome Back" greeting upon a returning End User device connecting to the WiFi;
 - 6.6.6 ability to redirect End Users to web addresses determined by the Customer based on the End User's device type; and
 - 6.6.7 a comfort branded message display to provide a smoother End User experience for slower connections.

- 6.7 The back end editing and reporting capability allows the Customer to:
- 6.7.1 upload images for the initial registration (landing) page;
 - 6.7.2 edit the re-direct URL's to direct traffic upon End User connection to the WiFi;
 - 6.7.3 add, delete and/or rename access points;
 - 6.7.4 configure campaigns;
 - 6.7.5 modify the initial registration (landing) page input fields; and/or
 - 6.7.6 configure portal flow by enabling or disabling specific pages.
- 6.8 In addition to the features set out in paragraph 6.7, the back end editing and reporting capability provides analytics for the information gathered by the front end captive portal as described in paragraph 6.6. This data might include:
- 6.8.1 date/time of registration/authentication;
 - 6.8.2 Customer Premises and access point used for registration/authentication;
 - 6.8.3 URL used to trigger the portal registration/authentication;
 - 6.8.4 End User device type used on registration/authentication; and
 - 6.8.5 browser type/End User agent used for registration for subsequent connections.
- 6.9 The reporting interface can segment the Customer's network into access points, Customer Premises and/or the wireless local area network. The features of the reporting interface are as follows:
- 6.9.1 dashboard view to give an overview of the day's activity;
 - 6.9.2 search functionality to locate a specific End User device and track their activity;
 - 6.9.3 ability to track an individual End User's connections and authentications on the Customer's network;
 - 6.9.4 graphs to provide an overview of the registrations, authentication and connections on a daily, weekly, monthly and yearly basis;
 - 6.9.5 reports detailing the top Customer premises, access points, redirections and access points;
 - 6.9.6 timeline graphs to provide a view of level of activity throughout the day;
 - 6.9.7 listing of all End User details gathered;
 - 6.9.8 an overview of the End User device types connected to the Customer's network; and
 - 6.9.9 exportation of all of the data captured by the front end captive portal for external reporting.

WiFi Engage Deliverables

- 6.10 The WiFi Engage Services includes the following one-off deliverables:
- 6.10.1 installation and implementation of the WiFi Engage Software onto equipment provided by Vodafone and located at the Customer Premises;
 - 6.10.2 configuration of the WiFi Engage Software to reflect the Customer's Wireless Local Area Network infrastructure, which may include:
 - (a) access points MAC addresses and descriptions;
 - (b) Customer Premises names;
 - (c) region details (if appropriate);
 - (d) wireless names; and
 - (e) standard landing pages.
 - 6.10.3 recommendations to the Customer for initial registration (landing) page design;
 - 6.10.4 Customer training for use of the WiFi Engage Software, which will include an initial face to face workshop followed by 4 (four) web based training sessions, which shall last not more than 2 (two) hours each; and
 - 6.10.5 support of Customer acceptance testing across an agreed selection of up to 5 (five) Customer Premises.
- 6.11 The WiFi Engage Services include the following on-going deliverables:
- 6.11.1 provision of WiFi Engage Software updates as and when they are available to the Company;
 - 6.11.2 telephone and web support between the hours of 09:00 and 17:00 on the next Business Day following receipt of the Customer queries, this support will include assistance with on-going configuration queries of the Customer;
 - 6.11.3 web based training of up to 4 (four) training sessions a year. This web based training is to be provided to those employees of the Customer who are responsible for configuring the WiFi Engage Software. This training is to be provided to a maximum of 6 (six) employees and shall last not more than 2 (two) hours each.

7 WiFi ENGAGE SOFTWARE

- 7.1 The Company grants to the Customer a non-exclusive, non-transferable, revocable licence for the Customer and the End Users to use the WiFi Engage Software and the Software Documentation at the Customer Premises for the Customer's internal business purposes only. The Customer agrees that any attempt to use the WiFi Engage Software or the Software Documentation by more than the specified number of uses shall constitute a material breach of this Contract.
- 7.2 The Customer shall effect and maintain adequate security measures to safeguard the WiFi Engage Software and Software Documentation from theft or unauthorised use. This section shall survive termination of the licence or this Contract.
- 7.3 The Customer shall not use the WiFi Engage Software contrary to any restriction set out in this Contract or otherwise in a way that is not expressly permitted by this Contract. The Customer's right to use the WiFi Engage Software and any Software Documentation shall not include the rights of any third party to use or have access to the WiFi Engage Software and any Software Documentation and in any event, the Customer shall ensure that all such use does not exceed the Customer's permitted use.

8 FRIENDLY WiFi

- 8.1 Where Friendly WiFi is identified in the Order Form as being procured, then this paragraph 8 shall apply.
- 8.2 The Licence terms set out in Appendix 1 to these Specific Conditions shall apply.

9 CUSTOMER OBLIGATIONS

- 9.1 Where the Supported Hardware and Software is located at the Customer Premises or another location (other than the Company's premises) the Customer shall:
- 9.1.1 provide reasonable on-site 'remote hands' assistance, including power cycling the Supported Hardware and Software, to troubleshoot and diagnose any issues;
 - 9.1.2 ensure that all Supported Hardware and Software is housed in an appropriately secure, well-ventilated cabinet with sufficient environmental control to maintain both heat and moisture within tolerable limits; and

- 9.1.3 ensure the power supply to the Supported Hardware and Software is protected to maintain continuous supply and prevent spikes and losses.
- 9.2 The Customer shall:
- 9.2.1 not configure, maintain or modify (or permit any third party to do so) any Supported Hardware and Software without the prior written consent of Company;
- 9.2.2 be responsible for any third party services or infrastructure it provides to enable the provision of the Local Area Network Services;
- 9.2.3 maintain subscriptions to vendor-specific software assurance programs for the duration of this Contract in respect of the Supported Hardware and Software; and
- 9.2.4 ensure that where any consents and/or agreement is required from the Customer under this Contract that such consent and/or agreement shall not be unreasonably withheld and will be provided in a timely manner.
- 9.3 The following Customer Obligations apply to the Local Area Network Services, and the Company shall have no liability for any failure to provide the Local Area Network Services (including failing to meet any Service Level) to the extent caused by:
- 9.3.1 any failure by the Customer to provide secure connectivity from the Company's management systems to the Supported Hardware and Software, which is required to enable remote configuration or management of the Supported Hardware and Software by the Company; and/or
- 9.3.2 any failure by the Customer to meet and satisfy any of its obligations set out in the Contract.
- 9.4 Where certificates are to be provided by the Customer to the Company for implementation, it is the responsibility of the Customer to provide the certificates in a timely manner in order for implementation prior to the expiry of the current certificate.
- 9.5 The Customer will nominate approved Customer Representatives who may log incidents and requests with the Company;
- 9.6 The Customer will provide to the Company relevant details of all previously completed triage and diagnostics testing (and results thereof) when raising a request for support in order for the Company's resources to review and factor into any further action required to be undertaken by the Company.
- 9.7 The Customer will provide all and any connectivity and remote access for the Company's resources to utilise if the Customer requires the Company's resources to directly access the Customer environment.

10 EXCLUSIONS

- 10.1 The following are excluded from the Local Area Network Services:
- 10.1.1 the cost of any software license renewals or security certificate renewals;
- 10.1.2 the provision or installation of hardware, licensing and/or security certificates that are required to meet the pre-requisites for any code upgrades released by the third party vendor;
- 10.1.3 the provision of product training and/or technical consulting services unless otherwise set out in the Order Form;
- 10.1.4 where the configuration of additional reporting is specified in this Contract, any ongoing support and management of these reports, or any operational responses based on the output of these reports;
- 10.1.5 management of Maintenance Services which are provided by a third party. The Company will on request pass relevant information in relation to Supported Hardware and Software to the third party but will not manage that third party's performance of its obligations. The Company shall have no responsibility or liability for the acts or omissions of third parties providing Maintenance Services;
- 10.1.6 monitoring or alerting on any security alerts and incidents;
- 10.1.7 unless included in IPS Policy Management, any interpretation of or recommendations regarding any security related logs or alerts arising from the Supported Hardware and Software including but not limited to intrusion prevention system (IPS) logs for firewalls;
- 10.1.8 incidents relating to the underlying infrastructure that the Supported Hardware and Software reside on, including the physical hardware; and
- 10.1.9 liaising with relevant third party vendors.
- 10.2 The Customer acknowledges and agrees that the WiFi Engage Services shall have certain specific exclusions set out below:
- 10.2.1 the Company will not provide any network capacity or connectivity to the Customer Premises from the public or carrier network;
- 10.2.2 the Company will not operate the Customer's WiFi network;
- 10.2.3 the Company will not provide the hosting of the WiFi Engage Services, Software, Software Documentation or related database;
- 10.2.4 the Company will not prepare analysis of the data provided by the WiFi Engage Services or the Software nor shall the Company run reports of the data;
- 10.2.5 the Company will not remotely monitor the WiFi Engage Services, WiFi Engage Software or Customer's WiFi network;
- 10.2.6 the Company will not provide advice in respect of End User Terms for use of the WiFi network or capture and use of the data from End Users; and
- 10.2.7 the Company will not be obliged to perform a back-up or otherwise replicate any of the content created by the Customer or any End User using the WiFi Engage Services or WiFi Engage Software.

11 SERVICE LEVELS

- 11.1 The Company will supply Service Desk, Change Management, Event Management, Incident Management and Problem Management to the extent required in accordance with the Local Area Network Services in accordance with Specific Conditions X3 – Standard Operational Services.

12 CHARGES

- 12.1 The Charges for the Local Area Network Services are as specified in the Order Form.
- 12.2 Unless otherwise indicated on the Order Form, the Charges will be invoiced annually in advance with the first invoice issued by the Company on or around the Commencement Date for the Local Area Network Services and annually thereafter.

13 FAIR USAGE POLICY

- 13.1 All Local Area Network Services are provided on a 'reasonable use' basis, as determined by the Company.
- 13.2 If, using its reasonable judgement, the Company considers that the use of the Local Area Network Services by the Customer has consistently or notably exceeded typical usage by other customers or that an individual Request made by the Customer is not reasonable in nature, the Company may take reasonable steps to address the usage pattern or Request. Such steps may include:
- 13.2.1 remedial work to address the root cause of the issues that are causing overuse of the Local Area Network Services, such work being chargeable by the Company on a time and materials basis;
- 13.2.2 revising recurring charges or imposing additional time and materials charges in consideration of the overuse/request;
- 13.2.3 limiting the Customer's use of the Local Area Network Services in line with typical customer use; and/or
- 13.2.4 implementation of or change to a Fair Usage Policy relating to the Local Area Network Services or to a particular element of the Local Area Network Services.
- 13.3 Use of the Local Area Network Services will be measured using a three (3) month rolling average.
- 13.4 The Charges for the Service Options "Essentials" and "Enterprise" will be compared against the quantity of hours purchased.
- 13.5 The Charges for the Service Option "Enterprise Plus" will be compared against the cost of the effort expended on delivering the "Enterprise Plus" Service Option as follows:

- 13.5.1 the Customer will be judged to have exceeded the Fair Usage Policy if its usage of the Service Option "Enterprise Plus" exceeds 120% of the Charges; and
- 13.5.2 a resource cost of £30 per hour will be used to determine the Customer's usage, which the Company reserves the right to amend at its reasonable discretion.

14 WiFi Protect Services

- 14.1 This paragraph 14 shall apply where WiFi Protect Services are referred to as being part of this Contract in the Order Form.
- 14.2 WiFi Protect Services are subscription-based and the Charges shall be on a per wireless access point basis. Set up Charges will be invoiced upon implementation of the WiFi Protect Services, as a one off and upfront cost, as set out in the Order Form.
- 14.3 The WiFi Protect Services are non-cancellable. If the Customer's use is beyond the cap set out in the Order Form ("**Overage**"), the Customer shall pay for such Overage.
- 14.4 The Customer shall comply and shall ensure that its End Users comply with the End User Licence Agreement available at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html.
- 14.5 The WiFi Protect Services include the following one-off deliverables:
- 14.5.1 the creation of the Customer account on the protect cloud service platform;
- 14.5.2 the creation of network identities; and
- 14.5.3 the creation and assignment of a content filtering and security policy.
- The creation of additional policies may incur additional charges.
- 14.6 The Company will supply Service Desk, Change Management, Event Management, Incident Management and Problem Management to the extent required in accordance with the WiFi Protect Services in accordance with Specific Conditions X3 – Standard Operational Services.

APPENDIX 1: FRIENDLY WIFI LICENCE

We, Daisy Corporate Services Trading Limited (Company Number 2888250) of One Central Boulevard, Blythe Valley, Shirley, Solihull, West Midlands B90 8BG ("the **Licensor**") non-exclusively license you ("the **Licensee**") to use:

- The registered trademark set out in Schedule 1 Part B of this Licence;
- The products referred to in Schedule 2 of this Licence;

1 DEFINITIONS

"Licence"	means the licence to use the registered trademark set out in Schedule 1 Part B and the products referred to in Schedule 2 in accordance with these Specific Conditions; and
"Licence Fee"	means the charges payable by the Licensee to the Licensor in connection with the Licence as set out in these Specific Conditions and described as Friendly WiFi Licence Fee.

2 GRANT

- 2.1 The Licensor hereby grants to the Licensee a non-exclusive Licence to use the trademark in their respective territory only, strictly in accordance with the terms and conditions set out in this Licence solely for the purpose of the participation by the Licensee in the Friendly WiFi certification.

3 TITLE, GOODWILL AND REGISTRATIONS

- 3.1 The Licensee acknowledges that the Licensor is a licensee of the trademark, licensed products and any associated Intellectual Property.
- 3.2 Any goodwill in the trademark and any associated Intellectual Property shall accrue to the Licensor.
- 3.3 The Licensee shall not do, or omit to do, or permit to be done, any act that will or may weaken, damage or be detrimental to the trademark or any associated Intellectual Property or the reputation or goodwill associated with the trademark and any associated Intellectual Property or the Licensor, or that may invalidate or jeopardise any registration of the trademark.
- 3.4 The Licensee shall not apply for, or obtain, registration of the trademark and/or any associated Intellectual Property for any goods or services in any country.
- 3.5 The Licensee shall not apply for, or obtain, registration of any trade or service mark in any country that consists of, or comprises, or is confusingly similar to, the trademark and/or any associated Intellectual Property.
- 3.6 The Licensee shall provide, at the request and expense of the Licensor, all necessary assistance required for maintaining any existing registrations of the trade mark and challenging any pending applications. The Licensor shall provide to the Licensee on request copies of receipts of any renewal fees.

4 LICENSOR'S WARRANTIES

- 4.1 The Licensor warrants that it is a licensee of the registered trademark and associated Intellectual Property set out in Schedule 1, the Licensor further warrants that it has the right to grant a licence in respect of the same.

5 LICENCE FEE, CHARGES AND INVOICING

Licence Fee

- 5.1 On the commencement of this licence and each subsequent anniversary for the duration of the Licence, any applicable Licence Fee shall be due.
- 5.2 On or before each date that the Licence Fee is due, the Licensee shall inform the Licensor of the current number of its sites and sizes, whether or not this number has changed from the previous year.
- 5.3 Should the Licensee increase the number of its sites and sizes at any time during the term of the Licence but between the dates that the Licence Fee falls due, the Licensee shall immediately inform the Licensor

Charges

- 5.4 The Licensee shall pay to the Licensor all Charges in accordance with the terms and conditions agreed between the Licensor and Licensee.
- 5.5 For the avoidance of doubt, no part of the Licence Fee or any Charges shall be refundable by the Licensor upon termination of the Licence for any reason whatsoever.

6 CONDITIONS OF USE

- 6.1 The Licensee shall be entitled to use the trademark and all associated Intellectual Property provided always that:
- (a) it has in place and is using and maintains use of the Minimum Filter Requirements set out within Schedule 3; and
- (b) it uses the trademark and all associated Intellectual Property strictly in accordance with the terms this Licence.
- 6.2 The Licensee shall display the trademark in a position that is clearly visible to its customers. This may be displayed in the form of signage or displayed electronically such as a WiFi landing page. Where used electronically, the mark must include a hyperlink to <https://www.friendlywifi.com>.

7 PROTECTION OF THE TRADEMARK AND ASSOCIATED INTELLECTUAL PROPERTY

- 7.1 The Licensee shall immediately notify the Licensor in writing giving full particulars if any of the following matters come to its attention:

- (a) any actual, suspected or threatened infringement of the trademark or associated Intellectual Property;
 - (b) any actual or threatened claim that the trademark or associated Intellectual Property are invalid;
 - (c) any actual or threatened opposition to the trademark or associated Intellectual Property;
 - (d) any claim made or threatened that use of the trademark or associated Intellectual Property infringes the rights of any third party;
 - (e) any person applies for, or is granted, a registered trademark by reason of which that person may be, or has been, granted rights that conflict with any of the rights granted to the Licensee under this Licence; or
 - (f) any other form of attack, charge or claim to which the trademark and/or associated Intellectual Property may be subject.
- 7.2 In respect of any of the matters listed in paragraph 7.1 of this Licence:
- (a) the Licensor shall, in its absolute discretion, decide what action if any to take;
 - (b) the Licensee shall grant control over, and conduct of, all claims and proceedings;
 - (c) the Licensee shall not make any admissions other than to the Licensor and shall provide the Licensor with all assistance that it may reasonably require in the conduct of any claims or proceedings; and
 - (d) the Licensor shall bear the cost of any proceedings and shall be entitled to retain all sums recovered in any action for its own account.
- 7.3 The provisions of section 30 of the Trade Marks Act 1994 (or equivalent legislation in any jurisdiction) are expressly excluded.

SCHEDULE 1 - TRADEMARK

Part A

Mark with Associated Intellectual Property



Part B

Registered Trade Marks

Mark	Registered? (Y/N)	Application or registration no.	Date of application or registration	Classes
Digital Friendly WiFi	Y	UK00003219129	16.03.17	42

SCHEDULE 2 - LICENSED PRODUCTS

Friendly WiFi display materials in various forms and variations in accordance with the brand guidelines, including but not limited to window stickers, electronically downloadable logos and table cards.

SCHEDULE 3 - MINIMUM FILTER REQUIREMENTS

The logo is to be displayed at venues of organisations who are licenced members of the Friendly WiFi scheme to inform customers and the general public that the WiFi service at the venue is filtered to meet the two levels of protection as specified below:

1 The standard public WiFi offering will automatically filter the IWF list.

This is a List of URLs (webpages) that depict indecent images of children, advertisements for or links to such content. The list typically contains 900 URLs at any one time and can vary between 600 and 1500 URLs. It is updated twice a day to ensure all entries are live.

2 The standard public WiFi offering will also include filters to block pornography and will use generally recognised list providers to filter pornography

This will help prevent children and young people from accessing inappropriate pornographic material themselves and should also limit accidental exposure to inappropriate material that nearby adults might be looking at in public.

The Licensor defines pornography as any content whose primary purpose is sexual arousal or stimulation. This content need not contain nudity. The Licensor may consider certain 'glamour' works to be pornographic.

Pornographic content will typically include:

- explicit images of real sexual activity (for example, masturbation, oral sex, penetration, ejaculation);
- sexual activity with graphic detail (for example, sight of genitalia or non-explicit images of masturbation, oral sex, penetration, ejaculation);
- sexual fetish material;
- very strong references to sexual behaviour using strong pornographic terms

(Such content may not be regarded as pornography if its primary purpose is not sexual arousal or stimulation.)

The Licensor will not consider as pornography detailed breast and genital nudity within a sexualised context provided the images (i) form part of a genuine sex education work and (ii) are present only for the purpose of education.

Provided condition (ii) above is met, The Licensor will not consider as pornography any genuine sex education and advice.

IWF (Internet Watch Foundation)

Information about becoming a Member of the IWF is found on their website at: www.iwf.org.uk/join-us