

# BT Assure DoS Mitigation UK

## Annex to the Internet Connect UK Schedule

### Contents

A note on 'we' and 'you' .....	2
1. Service Summary .....	2
2. Service Standard Components .....	2
3. Service Options .....	2
4. Service Management Boundary .....	4
5. Specific Terms and Conditions .....	4
6. Our Obligations .....	6
7. Your Obligations .....	6
8. Notification of Incidents .....	8
9. Invoicing .....	9
10. Cancellation Charges prior to the Service Start Date .....	9
11. Charges at the End of the Contract .....	9
12. Service Amendment .....	10
13. Service Availability .....	11
14. Defined Terms .....	12

## A note on 'we' and 'you'

'We', 'us' and 'our' mean BT.

'You' and 'your' mean the Customer.

Phrases that refer to 'either', 'neither', 'each of us', 'both of us' or 'we both' mean one or both Parties, whichever makes sense in the context of the sentence.

## Application of this Annex

The following terms and conditions will apply where you are contracting for the BT Assure DoS Mitigation Service. They apply in addition to:

- (a) Conditions contained within the Internet Connect UK Schedule to the General Terms; and
- (b) The Order.

Where this Annex varies any clause in the Internet Connect UK Schedule, the variation applies to the Services in this Annex only, unless expressly stated.

## Part A – The Service

### 1. Service Summary

We will provide to you a service that mitigates attacks by profiling normal Internet traffic behaviour and proactively monitoring the Internet traffic routing to your Internet connection. DDoS detects floods, worm and anomalous traffic behaviour; in these circumstances your traffic will be re-routed to the threat management system which will permit legitimate traffic to proceed. The Service is comprised of:

- 1.1 all of the service standard components set out in paragraph 2 as set out in any applicable Order; and
- 1.2 any of the service options set out in paragraph 3 that are selected by you as set out in any applicable Order,

(the "**Service**").

### 2. Service Standard Components

We will provide to you all of the following service standard components in accordance with the details set out in any applicable Order:

- 2.1 a cloud service which monitors Malicious Attacks, provided on our BT Network over the BT Internet Connect UK Service (unavailable on Internet connectivity from other ISPs) in the UK only;
- 2.2 a Service Centre available 24 hours a day, seven days a week including public holidays for you to report faults;
- 2.3 monitoring of traffic on Managed Object(s);
- 2.4 investigation of anomalous traffic patterns;
- 2.5 Alerts; and
- 2.6 weekly reports available to the you via the Portal of Alerts and traffic performance

### 3. Service Options

## DoS Mitigation Annex to the Internet Connect UK Schedule

We will provide to you the “Bronze”, “Silver” or “Gold” option that you select in the Order. These options relate to the respective specifications set out in the table below and in any applicable Order, and will apply in accordance with the details set out in that Order. All options provide automated detection of Malicious Attacks and automated mitigation on Managed Object(s). <b>Service option specification</b>	Service options		
	Bronze	Silver	Gold
Managed Object(s) – you will provide us with details of the Managed Object(s) via the Mitigation Template. The Service will provide access to the following for each Managed Object: <ul style="list-style-type: none"> <li>• Alerting Service;</li> <li>• weekly report; and</li> <li>• Portal.</li> </ul>	1 Managed Object	3 Managed Objects	5 Managed Objects
Traffic reports and Alert options available via the Portal.	Yes	Yes	Yes
Ability to modify the reports available via the Portal.	No	Yes	Yes
<b>Security Centre Resolver Group</b> - technical advice and support outside of a Malicious Attack or suspected Malicious Attack and any changes to the Mitigation Template.	No	Mon-Fri 9-5 (excluding bank holidays).  # Up to 16 changes to a Mitigation Template per annum is included within the price	24/7 (including bank holidays).  # Unlimited changes to a Mitigation Template is included within the price.

<p><b>Security Centre Resolver Group</b> – technical advice and support during a Malicious Attack, or suspected Malicious Attack.</p>	<p>Limited to initial set up.</p>	<p>24/7 (including bank holidays) access to the Security Centre Resolver Group.  automated and option of manual mitigation (and Alerts) as set out in paragraph 3 above.</p>	<p>24/7 (including bank holidays).  In addition to the automated mitigation (and Alerts) as set out in paragraph 3 above, we will,  (a) monitor the traffic on your Managed Objects; and  (b) investigate any unexpected traffic patterns;  (c) take any additional mitigation action required; and  (d) advise you of any action to take.</p>
<p>The following service options are available at an additional charge as detailed in the Order:</p>			
<p>Additional CPE for protection against Application Layer Attacks and in-depth, real-time attack reports detailing blocked hosts, origin countries of attacks and historic trends.</p>	<p>No</p>	<p>Yes</p>	<p>Yes</p>

**4. Service Management Boundary**

- 4.1 We will provide and manage the Service as set out in Parts B and C of this Schedule and as set out in the Order up to demarcation points as set out in the remainder of this paragraph 4 (“Service Management Boundary” or “SMB”).
- 4.2 For Service provided as a cloud service only (with no Additional CPE), the SMB , is detailed in paragraph 4.3 of Internet Connect UK Schedule.
- 4.3 For Service with Additional CPE, the SMB shall be:
  - 4.3.1 the ethernet port linking the Additional CPE to the Customer Router;
  - 4.3.2 the ethernet port linking the Additional CPE to your firewall; or
  - 4.3.3 where the Service is managed over the Internet - the ethernet port linking the BT Management Router to the Broadband Router.
- 4.4 We will have no responsibility for the Service outside the Service Management Boundary.
- 4.5 We do not make any representations, whether express or implied, about the interoperability between the Service and any Customer Equipment.

**5. Specific Terms and Conditions**

### 5.1 Minimum Period of Service

- 5.1.1 The Minimum Period of Service will be as set out in the Order and on expiry of the Minimum Period of Service the Contract will continue in force until terminated by either of us in accordance with the Contract.

### 5.2 Service option upgrades and downgrades

At any time, you may request a move from one of the options set out at paragraph 3 to another:

- 5.2.1 If you decide to upgrade to a higher service option, the following terms will apply:

- (a) no Termination Charges will be payable for the option that you are moving from;
- (b) we will re-calculate the Charges for the upgraded option; and
- (c) a new Minimum Period will apply to the upgraded option, which we will advise you of at the time of upgrading.

- 5.2.2 If you decide to downgrade to a lower Service option, the following terms will apply:

- (a) you will pay the Termination Charges for the option that you are moving from, as set out in paragraph 11 below;
- (b) we will recalculate the Charges for the downgraded option; and
- (c) a new Minimum Period will apply to the downgraded option, which we will advise you of at the time of downgrading.

### 5.3 Suspension and Termination

Where we believe that a Malicious Attack or frequent Malicious Attacks threaten the BT Network or are having a significant impact on our other customers:

- 5.3.1 we may (without Notice) prevent incoming traffic coming to the target of the Malicious Attack and deny traffic to that target to all areas of our BT Network, which may mean in some instances the target under attack may lose some or all Internet service;
- 5.3.2 we will make all reasonable efforts to keep you informed of reasons for suspension and anticipated timescale for resumption of service and to resume service as soon as possible; and
- 5.3.3 Where the Internet Connect UK Service provided under this Contract is terminated the BT Assure DoS Service will automatically terminate and you will pay the Termination Charges set out in paragraph 11 of this Annex, unless either party has terminated the Internet Connect UK Service under clause 18 of the Conditions.

### 5.4 Service Limitations

- 5.4.1 We will not be able to detect and mitigate all Malicious Attacks;
- 5.4.2 In some circumstances the mitigation may also filter out legitimate traffic;
- 5.4.3 We will not be liable for any failure to detect and/or mitigate any Malicious Attack or for filtering out legitimate traffic.

### 5.5 Charges and Deposits

- 5.5.1 The Charges for the Service will begin on the Service Start Date and are fixed for the Minimum Period of Service. All Charges will be calculated in accordance with the charging information attached to the Order.

## Part B – Service Delivery and Management

### 6. Our Obligations

#### 6.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Service, we will:

- 6.1.1 provide to you contact details for the helpdesk that you will be able to contact to submit service requests, report Incidents and ask questions about the Service (“**Service Centre**”);
- 6.1.2 comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at a Site and are notified to us in writing. We will not be liable if, as a result of any such compliance, we are in breach of any of our obligations under this Contract;
- 6.1.3 provide you with a date on which delivery of the Service (or each part of the Service, including to each Site) is due to start (“**Customer Committed Date**”) and will use commercially reasonable endeavours to meet any Customer Committed Date.

#### 6.2 Commissioning of the Service

Before the Service Start Date, we will:

- 6.2.1 configure the Service;
- 6.2.2 conduct a series of standard tests on the Service to ensure that it is configured correctly; and
- 6.2.3 on the date that we have completed the activities in this paragraph 6.2, confirm to you the Service Start Date.

#### 6.3 During Operation

On and from the Service Start Date, we:

- 6.3.1 in the event of a Malicious Attack being detected or advised to us:
  - (a) will provide automatic Alerts or advice by telephone (depending on the Service option chosen by you), including advice as appropriate on tests and checks to be carried out by you;
  - (b) carry out diagnostic checks from our premises; and
  - (c) will mitigate the Malicious Attack by:
    - (i) automatic intervention; or
    - (ii) manual mitigation (if agreed between us);
- 6.3.2 will maintain a web Portal to provide you with online access to performance reports;
- 6.3.3 may, in the event of a security breach affecting the Service, require you to change any or all of your passwords to the Portal; and
- 6.3.4 upgrade software/enhance functionality.

#### 6.4 The End of the Service

On termination of the Service by either one of us, or expiry, we will:

- 6.4.1 have the right to disconnect and remove any BT Equipment that may be located at the Site(s).

### 7. Your Obligations

#### 7.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Service by us, you will:

- 7.1.1 provide us with the names and contact details of any individuals authorised to act on your behalf for Service management matters (“**Customer Contact**”), but we may also accept instructions from a person who we reasonably believe is acting with your authority;
- 7.1.2 provide us with any information reasonably required without undue delay, including full details of the Managed Object(s);

- 7.1.3 advise us immediately of any changes to the Managed Object(s), authorised traffic and/or the contact details of the Customer Contact;
- 7.1.4 provide us with details of the Managed Object(s) via the Mitigation Templates;
- 7.1.5 complete and agree the Mitigation Template;
- 7.1.6 provide us with access to your Site(s) where necessary, during Business Hours, or as otherwise agreed, to enable us to set up, deliver and manage the Service and to respond to Incidents;
- 7.1.7 complete any preparation activities that we may request to enable you to receive the Services promptly and in accordance with any reasonable timescales;
- 7.1.8 notify us in writing of any health and safety rules and regulations and security requirements that apply at a Site;
- 7.1.9 maintain a PSTN, ISDN or broadband line(s) as required for the Additional CPE at the Site(s) for exclusive use with the Service.
- 7.1.10 provide a secure, continuous power supply at the Site for the operation and maintenance of the router and Additional CPE at such points and with such connections as we specify. In order to mitigate any Service interruption resulting from failure in the principal power supply, you will provide back-up power with sufficient capacity to conform to the standby requirements of the applicable British standards.

### 7.2 Service Operation

On and from the Service Start Date, you will:

- 7.2.1 take any steps that we advise you to take in the event of prolonged and frequent Malicious Attacks;
- 7.2.2 ensure that the Customer Contact reports Incidents and Malicious Attacks initially to the Service Centre using the reporting procedures agreed between both of us, and will be available for all subsequent Incident and Malicious Attack management communications;
- 7.2.3 immediately terminate access to any Customer Contact who ceases to be an authorised Customer Contact;
- 7.2.4 monitor and maintain any Customer Equipment connected to the Service or used in connection with a Service;
- 7.2.5 ensure that any Customer Equipment that is connected to the Service or that you use, directly or indirectly, in relation to the Service is:
  - (a) connected and used in accordance with any instructions, standards and safety and security procedures applicable to the use of that Customer Equipment;
  - (b) technically compatible with the Service and will not harm or damage BT Equipment, the BT Network, or any of our supplier's or subcontractor's network or Equipment; and
  - (c) approved and used in accordance with relevant instructions and Applicable Law;
- 7.2.6 immediately disconnect any Customer Equipment, or advise us to do so at your expense, if Customer Equipment does not meet any relevant instructions, standards or Applicable Law;
- 7.2.7 maintain a list of current Users and immediately terminate access for any person who ceases to be an authorised User;
- 7.2.8 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Service and:
  - (a) inform us immediately if a User ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;
  - (b) take all reasonable steps to prevent unauthorised access to the Service; and
  - (c) satisfy our security checks if a password is lost or forgotten.

7.2.9 if we request you to do so in order to ensure the security or integrity of the Service, change any or all passwords and/or other systems administration information used in connection with the Service.

### 7.3 The End of the Service

On termination of the Service by either one of us, or expiry, you will disconnect any BT Equipment or Additional CPE from the Service.

## 8. Notification of Incidents

8.1 Where you become aware of an Incident:

8.1.1 the Customer Contact will report it to our Service Centre;

8.1.2 we will:

- (a) give you a unique reference number for the Incident ("**Trouble Ticket**");
- (b) provide advice by telephone, including where appropriate advice tests and checks to be carried out by you;
- (c) where possible, carry out diagnostic checks from our premises and you will co-operate in diagnosing faults by carrying out any diagnostic and test routines requested by us or included in the manufacturer's instructions;
- (d) where the Incident is due to a fault in the Additional CPE and where we consider it necessary, and as soon as reasonably practicable, visit the Site where (b) and (c) do not diagnose or clear the Incident;

8.1.3 Where replacement parts are provided by us, the parts removed will become our property;

8.1.4 We may remove all or part of the Additional CPE from the Site for inspection, testing and repair, but whenever reasonably practicable we will take steps to protect the continuity of the Service.

8.1.5 We aim to respond to faults in the Additional CPE as follows:

Response Time	Restoration Time
4 hours	End of next Business Day

8.1.6 Break / Fix of BT Equipment within our Service Management Boundary will be next Business Day.

8.1.7 Incident Repair covers:

- (a) Incidents resulting from normal wear and tear; and
- (b) Incidents or work resulting from other causes or circumstances, but an additional charge will be payable. Such other causes or circumstances include:
  - (i) misuse; incorrect environmental conditions including incorrect temperature and humidity levels; faulty manufacture or design; mains electrical surges or failures; or
  - (ii) lightning damage; electromagnetic interference; any other accidental or deliberate damage.

8.1.8 Incident Repair does not cover:

- (a) loss of software programmes generated by you;
- (b) work at the your request outside of working hours;
- (c) repair, replacement or re-routing of your wiring or cabling or provision of additional wiring and cabling; or
- (d) Incidents reported by you which are not covered by Incident repair.

8.1.9 We will inform you when we believe the Incident is cleared, and will close the Trouble Ticket when:



- (a) you confirm that the Incident is cleared within 24 hours of being informed; or
- (b) we have attempted unsuccessfully to contact you, in the way agreed between both of us, in relation to the Incident and you have not responded within 24 hours of our attempt to contact you.

8.1.10 If you confirm that the Incident is not cleared within 24 hours of being informed, the Trouble Ticket will remain open, and we will continue to endeavour to resolve the Incident and, where appropriate, we will continue to measure availability downtime, until the Trouble Ticket is closed as set out in paragraph 8.1.9.

8.1.11 Where we become aware of an Incident, paragraph, 8.1.9 and 8.1.10 will apply.

### 9. Invoicing

9.1 We will invoice you for the Charges for the Service as set out in paragraph 9.1 in the amounts specified in any Orders:

9.2 Unless stated otherwise in an applicable Order, we will invoice you for:

9.2.1 the Recurring Charges for this Service as set out in the Order, monthly in advance;

9.2.2 Installation Charges, where applicable, on the Service Start Date;

9.2.3 Charges for the Professional Services where applicable for this Service, as set out in the Order, on the Service Start Date, or agreed during the term of the Contract;

9.2.4 any Termination Charges incurred in accordance with paragraph 10 upon termination of the relevant Service.

9.3 We may invoice you for any of the following Charges in addition to those set out in the Order:

9.3.1 Charges for providing the Professional Services outside of Business Hours;

9.3.2 Charges for investigating your reported Incidents where we find no Incident or that the Incident is outside the Service Management Boundary;

9.3.3 Charges for commissioning the Service as set out in paragraph 6.2 outside of Business Hours;

9.3.4 Charges for restoring Service if the Service has been suspended in accordance with clause 10.1.2 of the General Terms;

9.3.5 Charges for cancelling the Service in accordance with clause 17 of the General Terms;

9.3.6 Charges for expediting provision of the Service at your request after you've been informed of the Customer Committed Date; and

9.3.7 any other Charges set out in any applicable Order or otherwise agreed between both of us.

### 10. Cancellation Charges prior to the Service Start Date

10.1.1 If you cancel the Service prior to the Service Start Date, you will pay our reasonable costs, including the costs of any Equipment provided by or ordered from third parties, including our suppliers.

10.1.2 The Notice period in clause 17 of the General Terms (relating to cancelling an Order before the Service Start Date) is amended to 30 days.

### 11. Charges at the End of the Contract

If you exercise your right under clause 17 of the General Terms to terminate the Contract or any Service, for convenience, during the Minimum Period of Service, you will pay us Termination Charges by way of compensation, which will be:

11.1.1 all outstanding Charges for Service rendered;

11.1.2 an amount equal to 3 months' Recurring Charges;

11.1.3 any remaining Charges outstanding with regard to BT Equipment;

11.1.4 any waived Charges for the Professional Services;

11.1.5 De-Installation Charges (where applicable); and

11.1.6 during the first 12 months of the Minimum Period of Service only:

- (a) an amount equal to 100 per cent of the Recurring Charges for the part(s) of the Service terminated for any remaining months of the first 12 months of the Minimum Period of Service; and
- (b) any waived Installation Charges for the part(s) of the Service(s) that will be terminated.

11.2 On the last day of the Minimum Period of Service, we will invoice you for:

11.2.1 any outstanding Charges for Service rendered; and

11.2.2 De-Installation Charges (where applicable).

### **12. Service Amendment**

12.1 You may request, by giving us Notice, a change to:

12.1.1 an Order for the Service (or part of an Order) at any time before the applicable Service Start Date;  
or

12.1.2 the Service at any time after the Service Start Date.

12.2 If you exercise your right under paragraph 12.1, and except where a change results from our failure to comply with our obligations under the Contract, we will, within a reasonable time, provide you with a written estimate, including:

12.2.1 the likely time required to deliver the changed Service; and

12.2.2 any changes to the Charges due to the changed Service.

12.3 We have no obligation to proceed with any change that you request under paragraph 12.1, unless and until we have both agreed in writing on the necessary changes to the Charges, implementation timetable and any other relevant terms of the Contract to take account of the change.

12.4 If we change a Service prior to the Service Start Date because you have given us incomplete or inaccurate information, we may, in our reasonable discretion, apply additional reasonable one-time and/or Recurring Charges.

Part C – Service Targets

**13. Service Availability**

**13.1 Availability Service Targets**

From the Service Start Date, we will aim to provide the Service with target availability as follows:

13.1.1 99.95% availability at all times, subject to the terms of this Contract.

(the “**Availability Service Target**”).

## Part D – Defined Terms

### 14. Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the following meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule):

**“Additional CPE”** means any additional Equipment provided by us in connection with the provision of the Service.

**“Application Layer Attacks”** is a form of denial-of-service (DDoS attack) where attackers target the application layer of the Open Systems Interconnection model. The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack.

**“Alert”** means notification by us to you by email or any other means agreed between us of a Malicious Attack.

**“Availability Service Target”** has the meaning given in paragraph 13.1.

**“Broadband Router”** means the BT Internet Connect Service router.

**“BT Equipment”** means any equipment including any Additional CPE and software, other than Customer Equipment, used by us in connection with the provisions of the Service.

**“BT Internet Connect UK Service”** means the our data services that allow you to connect to the Internet using a range of access methods at a variety of speeds over the BT Network.

**“BT Management Router”** means a Cisco 1941 combined Router/Terminal Server or equivalent router.

**“BT Network”** means the communications network owned or leased by us and used to provide the Service.

**“Business Hours”** means between the hours of 0800 and 1700 in a Business Day.

**“Customer Committed Date”** has the meaning given in paragraph 6.1.3.

**“Customer Contact”** has the meaning given in paragraph 7.1.1.

**“Customer Equipment”** means any equipment including any software, other than BT Equipment, used by you in connection with a Service.

**“Customer Router”** means the Internet access router owned by you.

**“DDoS”** means Distributed Denial of Service.

**“De-installation Charges”** means the charges payable by you on de-installation of the Service that will be equal to the then current rates for Installation Charges on the date of de-installation.

**“Domain Name”** means a readable name on an Internet page that is linked to a numeric IP Address.

**“Equipment”** means BT Equipment and Customer Equipment.

**“Incident”** means an unplanned interruption to, or a reduction in the quality of, the Service or particular element of the Service.

**“Installation Charges”** means those Charges set out in the Order in relation to installation of the Service, Customer Equipment and/or BT Equipment as applicable.

**“Integrated Services Digital Network”** or **“ISDN”** means a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the PSTN.

**“Internet”** means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.

**“Internet Protocol”** or **“IP”** means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.

**“IP Address”** means a unique number on the Internet of a network card or controller that identifies a device to other devices on the Internet.

**“ISP”** means Internet Service Provider(s).

**“Local Area Network”** or **“LAN”** means the infrastructure that enables the ability to transfer IP services within Sites (including data, voice and video conferencing services).

**“Malicious Attack”** means a DDoS attack, DDoS flood, protocol misuse and behaviour anomaly based attack.

**“Managed Object”** means a range of IP addresses which we will monitor and thresholds that will be used to trigger an Alert and subsequently automated mitigation.

**“Minimum Period of Service”** means a period of 12 consecutive months beginning on the Service Start Date, unless otherwise set out in an Order.

**“Mitigation Template”** means the form which sets out the section of countermeasures that will be applied when the system goes into automatic or manual mitigation, and will be agreed by you and us.

**“Portal”** means a secure shared our website that enables you to view service information, request changes and download service reports.

**“Professional Services”** means assistance with the implementation, configuration of the Service and operational assistance.

**“PSTN”** means Public Switched Telephone Network, which is the concentration of the world’s public circuit switched telephone networks.

**“Recurring Charges”** means the monthly fees payable by you for the Service.

**“Security Centre Resolver Group”** means a team of security experts within us which are available to deal with any requests for assistance as set out in paragraph 3.

**“Service”** has the meaning given in paragraph 1.

**“Service Centre”** has the meaning given in paragraph 6.1.1.

**“Service Management Boundary”** has the meaning given in paragraph 4.1.

**“Site”** means a location at which the Service is provided.

**“Supported Equipment”** means the BT Management Router and the Additional CPE detailed on the Order. We may require the Supported Equipment to pass an acceptance test prior to the commencement of the Service.

**“Termination Charges”** means those Charges incurred in accordance with paragraph 10.

**“Trouble Ticket”** has the meaning given in paragraph 8.1.2.