1 Definitions and abbreviations

The following definitions and abbreviations shall apply, in addition to those in the General Terms and Conditions and the General Service Schedule:

"**Alert**" means notification of a Malicious Attack by BT to the Customer Contact by email or any other means agreed between the Parties.
"**Arbor**" means Arbor Networks Inc whose registered office is 76 Blanchard Road, Burlington, MA 01803 USA
"**Arbor Equipment**" means the Arbor APS Pravail which is Customer Equipment.
"**Arbor APS Pravail**" means Arbor Availability Protection System Pravail; the technology used by Arbor for this Service.
"**Associated Services**" means additional services, software and equipment required for the Service to function, which are not part of the Service itself. The required Associated Services are further specified in this Service Annex.
"**Broadband Router**" means an Internet router which is Customer Equipment.
"**BT Network**" means the communications network owned or leased by BT and used in connection with the Service.
"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.
"**Cisco Router**" means a Cisco 1941 combined Router/Terminal Server.
"**Customer Router**" means an Internet Access router which is Customer Equipment.
"**DDoS**" means Distributed Denial of Service.
"**Enabling Service**" has the meaning given in Paragraph 5.1.
"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Service or particular element of the Service.
"**Incident Repair**" means repair of a fault in the Supported Equipment which results in an Incident.
"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.
"**Internet Access Circuit**" means a link provided by the Customer to the Internet from the Customer Router which may be obtained from BT or another supplier.
"**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 and is visible by all other devices on the Internet.
"**IPSEC VPN**" means an encrypted VPN meeting IP communication protocol standard.
"**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.
"**Mitigation Template**" means the form which sets out the countermeasures that will be applied when the Service goes into automatic or manual mitigation as agreed between the Parties.
"**MPLS**" means multi-protocol label switching.
"**Professional Services**" means assistance with the implementation and configuration of the Service with the Enabling Services and operational assistance.
"**Protection Group**" means a range of IP addresses which BT will monitor and thresholds that will be used to trigger an Alert and subsequent mitigation.
"**Recurring Charges**" means the Charges for the Service or applicable part of the Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in the Order.
"**Service**" has the meaning given in Paragraph 2.
"**Service Desk**" means the BT helpdesk for any issues as further described in this Service Annex.
"**Severity Level 1**" means a Malicious Attack that has a serious impact on the IP Addresses applicable to the Protection Groups and which cannot be circumvented.
"**Severity Level 2**" means a Malicious Attack that has a large impact on a portion of IP Addresses applicable to the Protection Groups and which cannot be circumvented.
"**Severity Level 3**" means a Malicious Attack that has degraded the IP Addresses applicable to the Protection Groups and for which BT has been able to provide an alternative.
"**Severity Level 4**" means a minor Malicious Attack has occurred which has not impacted on the IP Addresses applicable to the Protection Groups.
"**Supported Equipment**" means the Cisco Router and the Arbor Equipment (being Customer Equipment) detailed on the Order and which has passed the agreed acceptance tests.
"**Ticket**" means a "**fault reference number**" as further described in this Service Annex.
"**Traffic**" means the flow of data across the Internet which is monitored by the Service.

"**Virtual Private Network**" or "**VPN**" means a network that appears private to your Users but is provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over the VPN are restricted to Sites belonging to your VPN.

2 Service Description

2.1 Service Summary

BT will provide to the Customer a 24 hours a day, 7 days a week Service that profiles normal internet Traffic behaviour to provide identification of Malicious Attacks based on anomalous Traffic patterns, to enable Malicious Attacks to be mitigated and filtered out. The Service is comprised of:

- all of the service standard components set out in Paragraph 2.2 and in any applicable Order; and
- any of the service options set out in Paragraph 2.3 that are selected by the Customer as set out in any applicable Order.

2.2 Service Standard Components

2.2.1 BT will provide to the Customer all of the following Service standard components in accordance with the details set out in any applicable Order:

- monitoring of Traffic on Protection Groups;
- investigation of anomalous Traffic patterns;
- mitigation support and advice;
- Alerts;
- weekly reports of Malicious Attacks and Traffic performance;
- administrative support;
- BT Service Desk support where Incidents will be logged and diagnosed;
- Incident Repair; and
- Professional Services up to a maximum of five (5) days.

2.2.2 Where a Malicious Attack has been detected by BT or reported by the Customer to the Service Desk, BT will:

- provide Alerts and/or advice by telephone to the Customer Contact including where appropriate advice on tests to be carried out by the Customer;
- carry out diagnostic tests from our premises; and mitigate the Malicious Attack by:
  - automatic intervention; or
  - manual intervention as agreed.
- respond to and use reasonable endeavours to apply mitigation to the Malicious Attack in accordance with the following table:

Severity of Malicious Attack	Target Response Time	Target Restoration Time
Severity Level 1	15 minutes	2 hours
Severity Level 2	1 hour	4 hours
Severity Level 3	1 hour	8 hours
Severity Level 4	1 hour	16 hours

2.2.3 **Notification of Incidents.** Incidents may be pro-actively detected by BT or reported by the Customer. Where the Customer experiences an Incident not yet detected by BT; the Customer Contact will report it to BT's Service Desk. For each Incident:

- BT will give the Customer a unique reference number for the Incident ("**Ticket**");
- BT will inform the Customer when BT believes the Incident is cleared, and BT will close the Ticket when:
  - the Customer confirms that the Incident is cleared within 24 hours of being informed; or
  - BT has attempted unsuccessfully to contact the Customer Contact, in the way agreed, in relation to the Incident and the Customer has not responded within 24 hours of BT's attempt to contact the Customer Contact.
- If the Customer confirms that the Incident is not cleared within 24 hours of being informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.
- Where BT can demonstrate the Incident is due to a fault in the Supported Equipment, BT will undertake an Incident Repair in accordance with Paragraph 2.2.4.

2.2.4 **Incident Repair.** To resolve Incidents, BT will:

- provide advice by telephone, including where appropriate advise the Customer of tests and checks to be carried out by the Customer; or
- carrying out diagnostic checks from Customer's premises.

- Where the actions set out in this Paragraph 2.2.4 do not clear the Incident BT will:
- visit the Site to diagnose and clear the Incident without undue delay; and
- remove all or part of the Supported Equipment from the Site for inspection, testing and repair, but whenever reasonably practicable BT will take steps to protect the continuity of the Service.

Incident Repair covers any fault in the Supported Equipment other than:

- loss of software programmes generated by the Customer;
- work at Customer's request outside of Business Hours;
- repair, replacement or re-routing of your wiring or cabling or provision of additional wiring and cabling;
- Incidents reported by the Customer which are not caused by a fault in Supported Equipment;

The Customer will:

- make available to BT any other Supported Equipment at the Site.

Where replacement parts are provided by BT, the parts removed will become BT's property.

2.2.5 **Suspension of Internet Service.** In the event BT reasonably determines that a Malicious Attack or frequent Malicious Attacks:

- threaten the BT Network; or
- are having a significant impact on BT's other customers,

BT shall prevent all incoming Traffic to the target of the Malicious Attack and deny Traffic to the target and to all areas of the BT Network. This may mean that the target of the Malicious Attack may lose some or all of their Internet service. BT shall will make all reasonable efforts to keep the Customer informed of the reasons for any suspension and any timescales for the removal of the suspension.

2.3 **Service Options**

Following options might be ordered by the Customer. Such shall be set out in any applicable Order and will be provided by BT in accordance with the details set out in that Order:

- Additional Professional Services on top of the Professional Services as set out in Paragraph 2.2 above.
- The provision of Supported Equipment. This shall be subject to separate terms for resale of BT Provided Equipment.

3 Service Delivery

3.1 BT will:

- provide to the Customer contact details for the helpdesk that the Customer will be able to contact to submit service requests, report Incidents and Malicious Attacks and ask questions about the Service 24 hours a day, 7 days a week ("**Service Desk**");
- configure the Service with the Enabling Services;
- conduct a series of standard tests on the Service to ensure that it is configured correctly;
- conduct acceptance tests on Customer Equipment where BT consider it necessary before including the Customer Equipment as Supported Equipment.

3.2 The Operational Service Date occurs on the date BT has completed above activities.

4 BT Service Management Boundary (SMB)

4.1 BT will provide and manage the Service as set out in this Service Annex and as further specified in the Order up to:

4.1.1 The ethernet port(s) linking the Arbor Equipment to the Customer Router and Customer firewall;

4.1.2 Where the Service is managed:

(a) over the Internet, the ethernet port linking the Cisco Router to the Broadband Router; or

(b) over MPLS, the ethernet port linking the Cisco Router to the other Enabling Services,

4.2 BT will have no responsibility for the Service outside the Service Management Boundary.

4.3 BT does not make any representations, whether express or implied, about whether the Service will operate in combination with any Customer Equipment or other equipment, Service and software not provided by BT.

4.4 **Service Limitations.** The Service is considered as an obligation of means; meaning that BT will not be able to detect and mitigate all Malicious Attacks. Furthermore, in some circumstances the mitigation may also filter out legitimate Traffic. Therefore BT's liability is limited to put in place the appropriate diligence and means to detect and/or mitigate any Malicious Attack or for filtering out legitimate Traffic as set out in this Service Annex; without commitment on result.

5 The Customer's Responsibilities

5.1 **Associated Services.** Before the Service can be delivered the Customer shall ensure that following Associated Services shall be in place to connect the Service and that these Associated Services shall comply with the minimum technical requirements:

- Customer Equipment including the Abor Equipment, Cisco Router and Broadband Router;
- Arbor Software;
- A Customer LAN;
- Internet Access Circuit; and
- Where the Service is managed over:
    - the Internet; IPSEC VPN between the Cisco Router and the Broadband Router; or
    - MPLS, a MPLS service.

(each an "**Enabling Service**").

If above Associated Services are provided by, these Associated Services(including, but not limited to any Enabling Service) then these Associated Services shall be subject to the respective terms and conditions as agreed between BT and the Customer for such Associated Services.

BT shall have no liabilities for providing the Service if these Associated Services are not in place before the delivery of this Service and BT may cancel the Service subject to the cancellation conditions as agreed in the General Terms and Conditions.

5.2 Before the Operational Service Date and, where applicable, throughout the provision of the Service, the Customer will:

- make available and maintain the Enabling Services and comply with the terms and conditions under which they are provided and pay all charges related to the use of the Enabling Services to the supplier of the Enabling Services;
- provide (in accordance with the General Service Schedule) BT with the names and contact details of any individuals authorised to act on your behalf for Service management matters ("**Customer Contact**");
- provide BT with any information reasonably required without undue delay including details of the Protection Groups via the Mitigation Templates;
- complete and agree the Mitigation Templates;
- ensure that the Customer Equipment has:
    - a publicly registered IP Address if the Service is to be managed via the Internet; or
    - IP Addresses allocated from your internal IP Address range if the Service is to be managed via MPLS; and
    - provide internal cabling between the Customer Equipment and Enabling Services, as appropriate.

5.3 On and from the Operational Service Date, the Customer will:

- advise BT immediately of any changes to the:
    - Customer Contacts or their contact details;
    - Enabling Services;
    - Protection Groups and authorised Traffic set out in the Mitigation Template;
- take any steps requested by BT in the event of a prolonged or frequent Malicious Attack;
- ensure that Users report Incidents or Malicious Attacks to the Customer Contact and not to the Service Desk;
- ensure that the Customer Contact will take Incident and Malicious Attack reports from Users and pass these to the Service Desk using the reporting procedures agreed between the Parties, and will be available for all subsequent Incident management and Malicious Attack communications;
- Immediately terminate access to any Customer Contact who ceases to be an authorised Customer Contact;
- monitor and maintain any Customer Equipment connected to the Service or used in connection with a Service;
- if requested by BT 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;
- take all reasonable steps to prevent unauthorised access to the Service; and
- co-operate in diagnosing Incidents by carrying out any diagnostics and test routines requested by BT or included in the manufacturer's instructions.

6 Charges and Payment Terms

6.1 The Charges for the Service will be set out in the Order, depending on the Service Option (as set out in Paragraph 2.3) selected.

6.2 Such Charges will be invoiced as set out in the General Service Schedule and paid in accordance with the payment terms as agreed in the General Terms and Conditions.

6.3 In addition, BT reserves the right to charge the Customer for any activities outside BT's Service Management Boundary and/or for investigating Incidents or Malicious Attacks reported by the Customer to BT where BT finds no Incident or Malicious Attack.

6.4 **Termination Charges.** In variance to what is agreed in the General Service Schedule; the following applies:

6.4.1 if the Customer terminates the Service for convenience or if BT terminates the Service for breach by the Customer before the Minimum Period of Service has expired, then, in addition to all outstanding charges for Service rendered, the Customer will pay the termination charges below:

(a) an amount equal to the Recurring Charges for the terminated Service for any remaining Months of the first 12 Months of the Minimum Period of Service;
(b) an amount equal to 20% of the Recurring Charges per Site for all other remaining Months of the Minimum Period of Service;
(c) any waived Professional Charges for the terminated Service; and
(d) De-installation Charges.

6.4.2 If the Customer terminates the Service at the end of the Minimum Period of Service or at any time thereafter, in addition to all outstanding charges for Service rendered, the Customer will pay only De-installation Charges.

7 Service Levels

There are no Service Levels applicable to this Service, hence the Service Levels as set forth in the General Service Schedule shall not apply to this Service.

8 Changes

8.1 Any changes to the Service which the Customer may require are subject to signature of a new Order whereby the Parties shall agree on the new applicable Charges, the required changes, implementation timetable and any other relevant changes to the terms to take account of the change.

9 Data Processing

9.1 Applicable terms. The Parties agree that it is anticipated that BT may receive or process Personal Data on behalf of the Customer as a Data Processor in connection to the Service or as a result of the provision of this Service. Any Customer Data is subject to the 'Data' clause as set out in the Agreement.

9.2 The nature and purpose of the Processing of Customer Personal Data. The Service provides protection against Distributed Denial of Service (DDoS) cyber attacks. No Personal Data is utilised by BT beyond that needed for provisioning, assurance and billing purposes. The Service operates at layer 3 and utilises IP Addresses. This in itself may not be Personal Data if the IP Address is allocated to a host or device, although the data may be "pseudonymised" i.e.: it could be possible for BT or the Customer to "triangulate" back to a location or an end User identifying usage behaviour. The DDoS Service identifies traffic or usage anomalies or patterns that could suggest an attack is commencing and then diverts the traffic to prevent it impacting the Customer networks, systems and applications. The traffic may be unwittingly generated from a device and IP Address belonging to any Data Subject.

9.3 The types of Customer Personal Data Processed by BT or its Sub-Processors or the Customer will be:

- website or IP address;

9.4 The Customer Personal Data will concern the following categories of Data Subjects:

- Customer employees;
- any Data Subject (as controlled by the Customer).

9.5 These lists are not exhaustive as the Customer will specify what Customer Personal Data is processed.