

BT Managed DDoS Security Service Schedule

Part A – Service Terms

Section A Service Terms

1. SERVICE SUMMARY

- 1.1** BT Managed DDoS Security is a service that reduces the risk of distributed denial of service "**DDoS**" attacks by profiling normal Internet traffic behaviour and proactively monitoring the Internet traffic routing to the Customer's Internet connection. The service can detect volumetric DDoS activity, and anomalous traffic behaviour and will instigate mitigation actions so that only legitimate traffic will proceed. BT does not guarantee that the Service will detect or block all Malicious Attacks and in some circumstances the mitigation actions carried out by BT may also filter legitimate traffic.
- 1.2** BT Managed DDoS Security has two variants:
- 1.2.1** BT Managed DDoS Security – Off BT's Network: offering a basic protection in the cloud; and
 - 1.2.2** BT Managed DDoS Security – On BT's Network: offering various service features and the option to purchase Security Devices.
- 1.3** Depending on what is selected by the Customer on the Order, the Off BT's Network and On BT's Network variants each have a separate Part B to this Schedule; setting out the:
- 1.3.1** the standard components of each Service variant; and
 - 1.3.2** any optional components of each Service variant as further detailed in an applicable Order, up to the point of the Service Management Boundary ("**Service**").
- 1.4** This Part A sets out the specific terms and conditions applicable to the Service, and Part B sets out the service description and the terms relating to how BT manages the Service.
- 1.5** This Schedule will not apply for the provision of any other services provided by BT (including the Enabling Services and sale of the Security Devices used in the provision of the Service) as such services will be governed by their separate terms and conditions.

2. MAINTENANCE, CHANGES AND SUSPENSION TO THE SERVICE

- 2.1** BT may carry out Planned Maintenance on the Service from time to time. BT will inform the Customer at least seven (7) calendar days in advance.
- 2.2** BT may change the Service provided the performance and quality of the Service is not materially adversely affected. Prior to introducing any change to the Service BT shall provide the Customer with as much notice as is reasonably practicable. Such changes may include:
- 2.2.1** introducing or removing features of the Service; or
 - 2.2.2** replacing the Service with a materially equivalent Service.
- 2.3** BT may occasionally suspend the Service in an event of emergency and/or to safeguard the integrity and security of its network and/or repair or enhance the performance of its network. Where possible, BT shall inform the Customer without undue delay in advance. Where it is not possible to inform the Customer in advance of restriction or suspension of any affected Service BT shall explain as soon as is reasonably practicable afterwards why such restriction or suspension was required.

3. GENERAL CUSTOMER OBLIGATIONS

- 3.1** The Customer will:
- 3.1.1** provide BT with the names and contact details of the Customer contact;

- 3.1.2 without undue delay provide BT with any information or assistance reasonably required by BT to enable it to comply with Applicable Law and perform its obligations hereunder with respect to the Service;
- 3.1.3 use the Incident reporting procedures notified to the Customer by BT, and ensure that the Customer operational contact is available for all subsequent Incident management communications;
- 3.1.4 ensure that the local area network ("LAN") protocols, applications and equipment used by the Customer are compatible with the Service;
- 3.1.5 complete any preparation activities that BT may request to enable the Customer to receive the Service promptly and in accordance with any agreed timescales;
- 3.1.6 procure services that are needed to permit the Service to operate, including Enabling Services as defined in Part B, and ensure they meet the minimum technical requirements specified by BT;
- 3.1.7 where the Customer has provided its own or a third party Enabling Service, ensure and confirm to BT that the Enabling Service is working correctly before reporting Incidents to BT;
- 3.1.8 inform BT of any planned maintenance on any third party provided Enabling Service;
- 3.1.9 provide service assurance support to BT, where reasonably requested, to progress the resolution of Incidents on an Enabling Service that is not being provided by BT;
- 3.1.10 in jurisdictions where an employer is legally required to make a disclosure to its Users and employees in relation to the Service:
 - (a) inform Users (individually or via local workers councils depending on Applicable Law) that as part of the Service being delivered by BT, BT may monitor and report the use of any targeted applications;
 - (b) ensure that Users have consented or are deemed to have consented to such monitoring and reporting (where such consent is legally required); and
- 3.1.11 be responsible for its Content and that of its Users (including any Content hosted by the Customer or any User on behalf of third parties).

4. CUSTOMER EQUIPMENT AND SITE REQUIREMENTS

- 4.1 If the Customer orders BT Managed DDoS – On Net with Managed DDoS Edge Defence, the Customer will:
 - 4.1.1 provide BT with any information reasonably required, without undue delay, and the Customer will ensure that the information is accurate and complete. In particular any information in relation to:
 - (a) to health and safety and the environment;
 - (b) details of the Managed Object(s) by completing the data capture document; and
 - (c) any changes to the Managed Object(s), authorised traffic and/or the contact details of the Customer contact.
 - 4.1.2 provide, at its own cost, any necessary internal cabling between the Security Device(s) and any other Customer equipment, including in particular the cabling between the NTU and the Security Device(s) at a Site;
 - 4.1.3 monitor and maintain any Customer equipment connected to the Service or used in connection with a Service;
 - 4.1.4 ensure that any Customer equipment that is connected to the Service or that the Customer uses, directly or indirectly, in relation to the Service:
 - (a) is correctly connected to Service;
 - (b) is adequately protected against viruses and other breaches of security;

- (c) will not harm or damage the Security Device(s), the BT Network, or any of BT's Suppliers' or subcontractors' network or equipment; and
 - (d) is approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer equipment;
- 4.1.5 immediately disconnect any Customer equipment, or advise BT to do so at the Customer's expense, where the Customer's equipment:
 - (a) does not meet any relevant instructions, standards or Applicable Law; or
 - (b) contains or creates material that is in breach of the Acceptable Use Policy and the Customer is contacted by BT about such material,and redress the issues with the Customer equipment prior to reconnection to the Service;
- 4.1.6 for Sites not under BT's control, get all the consents, licences, permissions and authorisations BT and the Customer need and keep them up to date so BT can provide the Service at the Sites, including for:
 - (a) making alterations to buildings;
 - (b) getting into property;
 - (c) dealing with local authorities, landlords or owners;
 - (d) installing equipment; and
 - (e) using the Service over the Customer's network or at a Site;
- 4.1.7 provide BT, or third parties acting on BT's behalf, with access to any Site(s) during Business Hours, or as otherwise agreed in an Order, to enable BT or its third parties, to set up, deliver, manage, maintain and restore the Service; and
- 4.1.8 ensure that the Customer or third parties, as required, configure routing/permissions on platforms or Enabling Services to allow BT to carry out the monitoring of the Internet traffic.

5. SOFTWARE LICENCE TERMS

- 5.1 The End User License Agreement ("**EULA**") establishes certain terms and conditions through direct privity of contract between the Customer and Supplier and as such the Customer will:
 - 5.1.1 be directly bound by the terms and conditions set out in the EULA contained in Part B and, where applicable, ensure that its Users also comply with the terms of the EULA;
 - 5.1.2 enter into the EULA for the Customer's own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between the Customer and the Supplier and the Customer will deal with the Supplier with respect to any loss or damage suffered by either of the Customer or the Supplier as such loss or damage will not be enforceable against BT; and
 - 5.1.3 observe and comply with the EULA for any use of the applicable Supplier software.
- 5.2 If the Customer does not comply with the EULA:
 - 5.2.1 BT may restrict or suspend the entire Service upon notice and:
 - (a) the Customer will continue to pay the Charges for the Service until the end of the Subscription Term; and
 - (b) BT may charge a re-installation fee to re-start the Service.
- 5.3 Where the EULA is presented in a 'click to accept' function and the Customer requires BT to configure or install software on their behalf, BT will do so as their agent and bind the Customer to the EULA. For this

purpose, the Customer hereby grants to BT a mandate to enter into the EULA in the Customer's name and on its behalf. BT and the Customer may also execute a power of attorney as part of the Order.

6. PASSWORDS, AUTHORISED USERS AND SECURITY

- 6.1 The Customer is responsible for the proper use of any usernames, personal identification numbers and passwords or similar used in conjunction with the Service, and the Customer will take all necessary precautions to ensure that the foregoing are kept confidential, secure and not made available to unauthorised persons.
- 6.2 The Customer will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Service.
- 6.3 The Customer will promptly terminate access of any person who is no longer an authorised User.
- 6.4 The Customer will promptly inform BT if a User's 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.
- 6.5 The Customer will change any or all passwords or other systems administration information used in connection with the Service if BT asks the Customer to do so in order to help safeguard the security or integrity of the Service.
- 6.6 The Customer will not allow any specific User license to be used by more than one User unless it has been reassigned in its entirety to another User.

7. IP ADDRESSES, DOMAIN NAMES

- 7.1 Except for IP Addresses expressly registered in the Customer's name, all IP Addresses and Domain Names made available by BT with the Service will at all times remain BT's ownership or the ownership of BT's Suppliers and are non-transferable.
- 7.2 All the Customer's rights to use BT IP Addresses or BT Domain Names will cease on termination or expiration of the Service.
- 7.3 The Customer warrants that they are the owner of, or are authorised by the owner of, the trade mark or name that the Customer wishes to use as Customer's Domain Name.
- 7.4 The Customer will pay all fees associated with registration and maintenance of the Customer's Domain Name, and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

Section B Acceptable Use Policy

8. INTRODUCTION

- 8.1 The Customer acknowledges that it has read and agrees to be bound by and to ensure that any Users will comply with this Section B ("**Acceptable Use Policy**" or "**AUP**").

9. USE OF THE SERVICE

- 9.1 The Customer will not use the Service in breach of Applicable Law or in any way that is considered to be:
 - 9.1.1 detrimental to any person or in a manner which violates or otherwise encroaches on the rights of others (including rights of privacy and free expression); and
 - 9.1.2 detrimental to the provision of services to the Customer or any other BT customer.
- 9.2 The Customer will not use the Service to intentionally take, or attempt to take, any action that could:
 - 9.2.1 transfer files that are, contain or are made up of viruses, Worms, Trojans, distributed denial of service, any back door or time-bomb or other harmful programmes or software designed to violate the security of BT, any other person or company; or

9.2.2 prevent, block or obstruct access to any programme installed on, or data saved in, any computer or damage or harm the operation of any of these programmes or the reliability or accuracy of any of this data.

9.3 Unless agreed in writing with BT:

9.3.1 the Customer will only use the Services for the commercial and business purposes for which they have been designed; and

9.3.2 the Customer will not modify, amend, change, reconfigure or otherwise repurpose all or any part of the Services for uses other than those pursuant to paragraph 9.3.1 above.

10. USE OF MATERIALS

10.1 The Customer will not create, download, receive, store, send, publish, transmit, upload or otherwise distribute any material, including information, pictures, music, video or data, that is considered to be:

10.1.1 harmful, immoral, improper, indecent, defamatory, offensive, abusive, discriminatory, threatening, harassing or menacing;

10.1.2 promoting or encouraging of illegal, socially unacceptable or irresponsible behaviour, or that may be otherwise harmful to any person or animal;

10.1.3 in breach of the intellectual property rights of BT or any other company or person, for example by using, distributing or copying protected or 'pirated' material without the express permission of the owner;

10.1.4 in breach of the privacy or data protection rights of BT or any other person or company; or

10.1.5 in contravention of any licence, code of practice, instructions or guidelines issued by a regulatory authority.

10.2 The Customer will ensure that all material that is derived from the machines or networks that it uses in connection with the Service is not in breach of this AUP.

11. SYSTEMS AND SECURITY

11.1 The Customer will not:

11.1.1 take any action that could:

(a) damage, interfere with, weaken, destroy, disrupt, harm, violate, disable, overburden, overtake, compromise, hack into or otherwise adversely affect any computer system, network or the internet access of the BT Network or network of any other person or company; or

(b) adversely affect or tamper with BT's security, the BT Network or any system or security network that belongs to any other person or company.

11.1.2 access any computer system or network belonging to any person or company for any purpose without permission, including to probe, scan or test the security of a computer system or network or to monitor data traffic;

11.1.3 connect the BT Network to machines, equipment or services that do not have adequate security protection or that are able to be used by others to carry out conduct that is not allowed by this AUP; or

11.1.4 collect, take or harvest any information or data from any BT services, BT's system or network or attempt to undermine any of BT's servers or systems that run BT services.

Section C Compliance and Regulation

12. EXPORT OF CONTENT USING CLOUD SERVICES

- 12.1** The Service comprises of a cloud service that utilises software and technology that may be subject to export control laws of various countries. The Customer is solely responsible for any compliance related to the way the Customer uses the Service and the location the Service is used including access by Users to the Service and for the Customer's Content transferred or processed using the Service, including any publication of such Content.

Section D Charges, Subscription Term and Termination

13. CHARGES

- 13.1** The Customer will pay the Charges for the Service and any optional features (including change requests) as specified in the Order.
- 13.2** In addition to the Charges set out in the Order, the Customer may be liable for the following additional Charges:
- 13.2.1** Charges for (de-)commissioning the Service outside of Business Hours;
 - 13.2.2** Charges for expediting provision of the Service at Customer's request after BT has informed Customer of the delivery date;
 - 13.2.3** Charges for investigating Customer reported Incidents where BT finds no Incident or that the Incident is outside the Service Management Boundary;
 - 13.2.4** Charges for restoring Service if the Service has been suspended by BT in accordance with the terms of the Governing Agreement; and
 - 13.2.5** Charges per element re-configured after the Operational Service Date must be agreed and documented in a new Order.

14. SUBSCRIPTION TERM AND TERMINATION

- 14.1** The Order sets out any Subscription Term (also called "**Minimum Period of Service**") applicable to the Service, as well as any associated volume commitments, invoicing terms and the termination Charges that are specific to the Service.
- 14.2** Unless otherwise agreed to the contrary, following the expiration of the Subscription Term, the Service shall continue unless and until terminated in accordance with the terms of the Governing Agreement referenced in the Order.

15. END OF SERVICE

- 15.1** On termination of the Service, Customer will:
- 15.1.1** retrieve all Customer data from the Service;
 - 15.1.2** provide BT with all assistance necessary to remotely decommission all network and applications supporting the Service at each customer Site(s);
 - 15.1.3** return to BT the software or intellectual property provided by BT and all copies of such.
 - 15.1.4** disconnect any Customer equipment (including the Security Devices) from the Service.
- 15.2** On termination of the Service BT will:
- 15.2.1** provide configuration information relating to the Service provided at the Site(s) in a format that BT reasonably specifies;
 - 15.2.2** decommission all network and applications supporting the Service at each Customer Site(s);
 - 15.2.3** where permitted under applicable mandatory law, delete any Content, including stored logs or any configuration data relating to BT's management of the Service.



Section E Data Protection

With this Service BT and its Suppliers will only act as Controller in accordance with the terms set out in the Governing Agreement.

Section F Defined Terms and Abbreviations

For the purposes of this Schedule defined terms and abbreviations shall have the meaning ascribed to them within the body of the Schedule or below:

“**Acceptable Use Policy**” means the policy as set out at Part A, Section B.

“**Acceptance Tests**” means those objective tests conducted by the Customer that when passed confirm that the Customer has accepted the Service and that the Service is ready for use save for any minor non-conformities that will be resolved as an Incident.

“**Application Layer Attacks**” is a form of denial-of-service 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 BT to the Customer by email or any other means as agreed of a Malicious Attack.

“**Applicable Laws**” means the laws as set out in the Governing Agreement as may be amended from time to time.

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

“**Business Day**” means generally accepted working days at the locality of the Site, excluding any national or bank holidays.

“**Business Hours**” means between the hours of 0800 and 1700 in a business day at the locality of the specific Site.

“**Charges**” means the charges applicable to this Service as set out on the Order.

“**Content**” means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

“**Controller**” shall have the meaning given to it in the GDPR.

“**CSP**” means the Customer Security Policy; containing the security rules, set and owned by the Customer, that are applied to the Service and determine the operation of the Service.

“**Customer Personal Data**” means any Personal Data Processed as a Processor by BT in the context of providing the Services under this Governing Agreement.

“**Data Subjects**” shall have the meaning given to it in the GDPR.

“**DDoS**” means Distributed Denial of Service, a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

“**DDoS Attack**” means an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.

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

“**Enabling Services**” means the services as defined in Part B – Service Description.

“**Ethernet**” means a technology for connecting devices in a wired local area network (“LAN”) or wide area network (“WAN”). It enables devices to communicate with each other via the IEEE 802.3-2008 protocol, which is a set of rules or common network language.

“**Fast Floods**” means a Service feature by which a DDoS Attack can be detected quicker and mitigations commenced quicker resulting with less delay and Service impact.

“**Flood**” means when a Router uses in a computer network a nonadaptive routing algorithm to send an incoming packet to every outgoing link except the node on which the packet arrives.;.

“**High Alert**” means when a high level of traffic is received within a particular period which indicates a likelihood that a customer may be under a DDoS Attack.

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679 (“EU GDPR”) and any amendment or replacement to it, (including any corresponding or equivalent national law or regulation that implements the GDPR as applicable to the Processing).

“**Governing Agreement**” means the general terms and conditions which govern this Schedule.

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

“**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.

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

“**Managed Object**” means a range of IP Addresses that BT will monitor and thresholds that will be used to trigger an alert and subsequently automated mitigation.

“**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 between the Parties.

“**Network Terminating Unit**” or “**NTU**” means the socket where the Customer’s wiring, equipment or existing qualifying data service is connected to the internet connection at the Site.

“**Operational Service Date**” means the date upon which the Service is made operationally available to the Customer at a Site and may be called the “**Service Start Date**” in some Governing Agreements.

“**Order**” means means an Order that accompanies a Service Schedule for a new Service and contains the Parties agreement on Charges, rate card (where applicable) and any other relevant commercial information related to the Service referred to in the Order.

“**Personal Data**” shall have the meaning given to it in the GDPR.

“**Planned Maintenance**” means scheduled maintenance that is planned in advance.

“**Portal**” means one or more webpages made available to the Customer by BT to provide for one or more specific functions in relation to the Service.

“**Priority 1 Problem**” means a security problem which cannot be circumvented and which also constitutes a complete loss of the Service.

“**Processing**” and “**Processor**” shall have the meaning given to it in the GDPR.

“**Reach-In**” means that in addition to the automated mitigation and Alerts, BT can be contacted to assist and support the Customer who is either under attack or in fear that it will be attacked.

“**Reach-Out**” means that in addition to the automated mitigation and Alerts, BT will actively monitor the traffic on the Customer’s network and pro-actively investigate any High Alerts and advise the Customer of any action to take.

“**Router**” means an equipment located at a Customer Site and used for routing traffic towards the internet.

“**Security Device**” means the equipment required on Site if the Customer orders BT Managed DDoS – On Net with BT Managed DDoS Edge Defence.

“**Security Operations Centre**” means the BT team supporting cyber security monitoring for the Customer.

“**Service Desk**” means the helpdesk that the Customer is able to contact to submit service requests, report incidents and ask questions about the Service 24x7x365 days.

“**Site**” means the physical Customer location to which the Service will be provided. Such Site may be Customer or third party owned.

“**Sub-Processor**” means a BT Affiliate or BT’s Supplier or subcontractor that BT engages to Process Customer Personal Data for the purposes of this Governing Agreement.



“**Subscription Term**” means the term contracted for this Service as set out in the Order. In some Governing Agreements this may also be called “**Minimum Period of Service**”.

“**Supplier**” means-Netscout Inc, 310 Littleton Road Westford, MA 01886-4105 USA.

“**User**” means any person who is permitted by the Customer to use or access a Service.