

## BT Managed Firewall Service Schedule Part A – Service Terms

### Section A Service Terms

#### 1. SERVICE SUMMARY

- 1.1** BT's Managed Firewall provides the Customer with network protection and optimisation at a Customer Site or hosted at a BT Site. The Customer can control inbound and outbound access to the Internet and control inbound traffic according to tightly controlled exceptions (firewall), managing Users' outbound web access according to pre-defined policy (URL filtering), and scanning traffic to block Malware. BT's Managed Firewall service comprises:
- 1.1.1** the standard components of the Service set out in Part B; and
  - 1.1.2** any optional components described in Part B and set out in any applicable Order, up to the point of the Service Management Boundary ("**Service**").
- 1.2** The Service is designed with a differentiated three-tier managed service proposition called Foundation, Foundation Plus and Premium (each a "**Graded Service Tier**") as further detailed in Part B and as set out in the Order. The Service is only available with one of the four Suppliers as set out in the Definitions.
- 1.3** During the Subscription Term the Customer may upgrade the selected Graded Service Tier to a higher Graded Service Tier (subject to a new Order and agreement on adjusted Charges).
- 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) as such services will be governed by their separate terms and conditions.

#### 2. MAINTENANCE, CHANGES AND SUSPENSION TO THE SERVICE

- 2.1** BT or the Supplier may carry out Planned Maintenance on the Service from time to time. BT will inform the Customer at least five (5) Business Days in advance when it concerns BT Planned Maintenance.
- 2.2** BT or the Supplier 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;
  - 2.2.2** replacing the Service with a materially equivalent Service; and
- 2.3** BT may occasionally suspend the Service in the event of an emergency and/or to safeguard the integrity and security of the Service, and/or repair or enhance the performance of the Service. 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 advise the Customer 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 relevant Customer contacts;
  - 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 to perform its obligations with respect to the Service;
  - 3.1.3** retain responsibility for the CSP;

- 3.1.4** use the Incident reporting procedures notified to the Customer by BT, and ensure that the Customer contact is available for all subsequent Incident management communications;
- 3.1.5** ensure that Users report Incidents to the Customer's designated point of contact and not directly to BT;
- 3.1.6** complete any preparation activities that BT may request to enable the Customer to receive the Service promptly and in accordance with any agreed timescales;
- 3.1.7** 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 or the Supplier;
- 3.1.8** 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;
- 3.1.9** inform BT of any Planned Maintenance on any third party provided Enabling Service;
- 3.1.10** provide service assurance support to BT, where reasonably requested, to progress the resolution of Incidents for any BT Service installed on an Enabling Service that is not being provided by BT;
- 3.1.11** 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);
- 3.1.12** share with BT any relevant internal processes or policies that may affect delivery of the Service, and operations, and BT will advise where these are not compatible with the Service;
- 3.1.13** make available to BT sufficient resources to facilitate ordering, design, and implementation of the Service;
- 3.1.14** ensure that the LAN protocols and applications used will be compatible with the Service;
- 3.1.15** manage, and provide BT with accurate details of Customer's internal IP Address design;
- 3.1.16** register any required Internet domain names using legitimate addresses which are public, registered and routed to the Site;
- 3.1.17** modify Customer's network routing to ensure appropriate traffic is directed to the Security Appliances, as switches provided as part of the Service only provide direct physical connectivity between Security Appliances and are not intended to support any network routing functionality;
- 3.1.18** ensure that Security Appliances are able to receive updates, such as Vulnerability signatures, directly over the Internet, or over an alternative path agreed with BT for that purpose;
- 3.1.19** obtain and provide in-life support for any Software running on the Security Appliances;
- 3.1.20** where necessary, provide and manage physical or virtual servers on the Site to a specification that BT agrees to run any Software that BT provides;
- 3.1.21** permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Security Appliances in its entirety and exchange it with a functioning replacement. BT will ensure that any data on the recovered appliance or components is rendered unreadable prior to disposal or recycling;
- 3.1.22** unless otherwise agreed on the Order, be responsible for implementing any Mitigation Action using the Portal(s); and
- 3.1.23** If the Customer orders the Co-Management option as set out in Part B, be responsible for:

- (a) ensuring that the Customer's authorised nominated Users complete the Portal(s) training available from the Supplier, before these Users are allowed to implement Simple Service Requests; and
- (b) if a Simple Service Request implemented by any User using the RBAC Profile has resulted in an Incident, notifying BT about the Security Incident.

**3.2** As the Customer is deemed to have approved all changes to the Customer security policy(ies) that are submitted to BT, BT shall not be liable for any disruption or loss to the Customer's business as a consequence of any misspecification by the Customer's security requirements implemented by BT.

#### 4. SPECIFIC CUSTOMER OBLIGATIONS

**4.1** The Customer will:

- 4.1.1** if an Out of Band Access modem is not included as part of the Service, agree an appropriate alternative with BT to allow for fault diagnosis and base configuration, allowing BT to establish in-band control of the Security Appliance, at the time of installation and following a failure of the Security Appliance;
- 4.1.2** if the connectivity to a Site is not provided by BT, ensure that the MPLS/Internet access circuit bandwidth is sufficient to meet Customer's requirements and the requirement for in-band management access from BT;
- 4.1.3** if the CSP production Service Option was not ordered; the Customer needs to submit a CSP that meets the requirements and specifications advised by BT at least 28 Business Days before the planned delivery date, including specifications that cover Customer's legacy network, application services and other Enabling Services, using the CSP requirements template provided by BT. BT will assess the CSP submitted and respond (if required) with an changed CSP, which will in turn be authorised by the Customer at least 10 Business Days before the planned delivery date;
- 4.1.4** if the Service is provided using existing Customer Equipment whereby BT takes over the management as set out in Part B;
  - (a) ensure that the Customer Equipment is working correctly. If it is discovered to be faulty before the Operational Service Date:
    - (i) the Customer will be responsible for resolving any faults;
    - (ii) agreed installation dates or Customer Committed Date(s) may no longer apply; and
    - (iii) additional Charges will need to be agreed if additional Site visits are required;
  - (b) ensure that the Customer Equipment is upgraded or replaced (hardware or software) if it becomes End of Life in accordance with BT's or Supplier's recommendations as BT will not support Customer Equipment which is End of Life.
  - (c) provide access to BT to any licence user centre, existing support contracts, authorisation code(s) or other information required by specific vendors and provided at the time of provision for registering products; and
- 4.1.5** if the Service is provided using existing Customer Equipment with Service Wrap only as set out in Part B;
  - (a) remain responsible for the provide and install any Customer Equipment as advised by BT,
  - (b) remain responsible for any support on hardware, software and applicable licensing agreements; including reporting to the third party vendor any Technical Incidents as notified by BT.
- 4.1.6** if the Service is provided with Vulnerability notification and Patching Service Option,
  - (a) identify and provide the name and contact details for a nominated representative responsible for liaising with BT;

- (b) advise BT if the Nominated Representative changes and ensure that BT has the current details of the Nominated Representative;
- (c) ensure that the Nominated Representative will:
  - (i) request implementation of Patches for each affected Security Appliance for the Vulnerability Notification and Patching Service Option;
  - (ii) agree a time slot with BT for the implementation of such Patches;
  - (iii) assess the suitability for deployment of the Patches that BT advises are available to address notified Vulnerabilities within your specific environments and for any post-implementation testing; and
  - (iv) request and authorise that the Patch is reversed out in the event that the Patch introduces issues;

## 5. CUSTOMER EQUIPMENT

### 5.1 The Customer will:

- 5.1.1 provide BT with any information reasonably required, including information in relation to health and safety and the environment, without undue delay, and the Customer will ensure that the information is accurate and complete;
- 5.1.2 provide, at its own cost, any necessary internal cabling between the BT Equipment and any Customer equipment, including in particular the cabling between the NTU and any Security Appliances at a Site;
- 5.1.3 monitor and maintain any other Customer equipment than the Security Appliances connected to the Service or used in connection with a Service;
- 5.1.4 ensure that any other Customer equipment than the Security Appliances is connected to the Service or that the Customer uses, directly or indirectly, in relation to the Service:
  - (a) is connected as recommended by BT;
  - (b) is adequately protected against viruses and other breaches of security;
  - (c) will not harm or damage BT Equipment, 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;
- 5.1.5 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.
- 5.1.6 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; and

- 5.1.7** 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.

## 6. SOFTWARE LICENCE TERMS

- 6.1** 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:
- 6.1.1** 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;
  - 6.1.2** 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
  - 6.1.3** observe and comply with the EULA for any use of the applicable Supplier Software.
- 6.2** If the Customer does not comply with the EULA, BT may restrict or suspend the entire Service upon notice. Where BT has exercised its right under this Paragraph 5.2:
- 6.2.1** the Customer will continue to pay the Charges for the Service until the end of the Subscription Term; and
  - 6.2.2** BT may charge a re-installation fee to re-start the Service.
- 6.3** Where the EULA is presented as 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 grants to BT a mandate to enter into the EULA in the Customer's name and on its behalf. For this purpose, BT and the Customer may for also execute a power of attorney as part of the Order.

## 7. PASSWORDS, AUTHORISED USERS AND SECURITY

### 7.1 Obligations applicable to any User.

- 7.1.1** The Customer will:
- (a)** be responsible for the proper use of any usernames, personal identification numbers and passwords used with the Service, and the Customer will take all necessary precautions to ensure these are kept confidential, secure and not made available to unauthorised persons;
  - (b)** will distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Service, including the Portal;
  - (c)** promptly terminate access of any person who is no longer an authorised User;
  - (d)** 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;
  - (e)** 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 ensure the security or integrity of the Service; and
  - (f)** 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.

### 7.2 Obligations applicable to Administrator(s).

- 7.2.1** BT will provide the Customer Administrator access rights to the Portal(s) as set out in Part B. The Customer will:

- (a) request, if applicable, up to five login/password combinations for access to a Portal for use by the Customer Administrator or its agents. The Customer Administrator may assign one login combination to BT's personnel;
- (b) not remove or alter the Administrator account without BT's prior consent;
- (c) avoid unauthorised access to the Administrator account;
- (d) keep the Administrator account password secure, change the password if the employee who has access to the Administrator account leaves the business, changes role and/or no longer requires access;
- (e) pay all remedial costs if there is an Incident which is a direct result of authorised or unauthorised access to the Administrator account and BT is requested to restore Service to the prior configurations;
- (f) where the Customer allows multiple Administrators to access the Portal(s), give each of the Administrators a unique login and provide management access or read only privileges specific to each of them and inform any additional Administrator of their responsibilities set out in this Schedule;
- (g) keep personnel access to the Administrator account up to date; and
- (h) keep records of any changes and make these available to BT where required.

**7.3** If the Customer fails to comply with this Paragraph 7.2, BT reserves the right to remove the Customer's administration rights.

## **8. BT EQUIPMENT**

**8.1** Where BT provides Security Appliances as BT Equipment to the Customer that is owned by BT as part of the provision of the Service, the Customer will:

- 8.1.1** keep the BT Equipment safe and secure;
- 8.1.2** only use the BT Equipment, or allow it to be used, in accordance with the instructions that BT may provide from time to time and only for the purpose for which it is intended to be used;
- 8.1.3** not move the BT Equipment or any part of it from the Site(s) without BT's written consent and the Customer will pay BT's costs and expenses reasonably incurred as a result of such move or relocation;
- 8.1.4** not make any alterations or attachments to, or otherwise interfere with, the BT Equipment nor permit any person (other than a person authorised by BT) to do so, without BT's prior written consent and, if BT gives its consent, agree that any alterations or attachments are part of the BT Equipment;
- 8.1.5** not sell, charge, assign, transfer or dispose of, or part with possession of the BT Equipment;
- 8.1.6** not allow any lien, encumbrance or security interest over the BT Equipment, nor pledge the credit of BT for the repair of the BT Equipment or otherwise;
- 8.1.7** not claim to be owner of the BT Equipment and to ensure that the owner of the Site(s) upon which the BT Equipment is located will not claim ownership of the BT Equipment, even if the BT Equipment is physically attached to the Site(s);
- 8.1.8** carry full replacement value insurance against any damage to or theft or loss of the BT Equipment;
- 8.1.9** in addition to any other rights that BT may have, reimburse BT for any losses, costs or liabilities arising from Customer's use or misuse of the BT Equipment or where the BT Equipment is damaged, stolen or lost, except where the loss or damage to BT Equipment is a result of fair wear and tear or caused by BT and its agents acting on BT's instructions;
- 8.1.10** ensure that BT Equipment appears in BT's name in the Customer's accounting books; and



- 8.1.11** in the event that there is a threatened seizure of the BT Equipment, or in the event that an insolvency event applies to Customer, immediately provide BT with notice so that BT may take action to repossess the BT Equipment.

## 9. IP ADDRESSES, DOMAIN NAMES

- 9.1** Except for IP Addresses expressly registered in the Customer's name, all IP Addresses and Domain Names made available by BT or the Supplier with the Service will at all times remain BT's ownership or the ownership of BT's suppliers and are non-transferable.
- 9.2** All the Customer's rights to use BT or the Supplier IP Addresses or Domain Names will cease on termination or expiration of the Service.
- 9.3** The Customer warrants that they are the owner of, or are authorised by the owner of, the trademark or name that the Customer wishes to use as Customer's Domain Name.
- 9.4** 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.

## 10. CUSTOMER TRANSACTION LOGS

- 10.1** BT and the Supplier may use, reproduce, store, modify, and display the information from the Customer transaction logs for the purpose of providing the Service.
- 10.2** BT and the Supplier may, use the Malware, Spam, Botnets or other information related to the Service for the purpose of:
- 10.2.1** maintaining and improving the Service;
  - 10.2.2** complying with all legal or contractual requirements;
  - 10.2.3** making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service;
  - 10.2.4** anonymously aggregating and statistically analysing the content; and
  - 10.2.5** other uses related to the analysis of the Service.

## 11. SUGGESTIONS, IDEAS AND FEEDBACK

- 11.1** The Customer agrees that the Supplier and/or BT will have the right to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by the Customer relating to the Service, to the extent it is not the Customer's confidential information.

## Section B Acceptable Use Policy

### 12. INTRODUCTION

- 12.1** 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**").

### 13. USE OF THE SERVICE

- 13.1** The Customer will not use the Service in breach of Applicable Law or in any way that is considered to be:
- 13.1.1** 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
  - 13.1.2** detrimental to the provision of services to the Customer or any other BT customer.

- 13.2** The Customer will not use the Service to intentionally take, or attempt to take, any action that could:
- 13.2.1** 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
  - 13.2.2** 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.

#### **14. USE OF MATERIALS**

- 14.1** 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:
- 14.1.1** harmful, immoral, improper, indecent, defamatory, offensive, abusive, discriminatory, threatening, harassing or menacing;
  - 14.1.2** promoting or encouraging of illegal, socially unacceptable or irresponsible behaviour, or that may be otherwise harmful to any person or animal;
  - 14.1.3** 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;
  - 14.1.4** in breach of the privacy or data protection rights of BT or any other person or company; or
  - 14.1.5** in contravention of any licence, code of practice, instructions or guidelines issued by a regulatory authority.
- 14.2** 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.

#### **15. SYSTEMS AND SECURITY**

- 15.1** The Customer will not:
- 15.1.1** 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.
  - 15.1.2** 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;
  - 15.1.3** 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
  - 15.1.4** 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

### 16. PROVISION OF THE SERVICE TO SITE(S) IN CHINA

- 16.1** The Customer accepts the risk that, due to changing nature of the China domestic and international landscape, the Service may have to be altered, suspended or even discontinued, resulting in degradation or full loss of connectivity which BT will not be responsible for.
- 16.2** BT may terminate and/or suspend the Service at any time in a Force Majeure Event and/or in accordance with applicable Chinese laws, regulations and/or directions from the Chinese authorities. BT will not be liable for any service credits, damages, and/or loss (whether direct or indirect) resulting from the termination or suspension of the Service in accordance with this Paragraph 16 (Provision of the Service to Site (s) in China).

## Section D Charges, Subscription Term and Termination

### 17. CHARGES

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

### 18. SUBSCRIPTION TERM, TERMINATION AND RENEWAL

- 18.1** 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.
- 18.2** 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.

### 19. END OF SERVICE

- 19.1** On termination of the Service, the Customer will:
- 19.1.1** retrieve all Customer data from the Service;
  - 19.1.2** provide BT with all assistance necessary to remotely decommission all applications supporting the Service;
  - 19.1.3** remove all Software associated with the Service for Customer's Security Appliances used in connection with the Service;
  - 19.1.4** disconnect any Customer equipment from the BT Equipment;
  - 19.1.5** not dispose of the BT Equipment other than in accordance with BT's written instructions; and
  - 19.1.6** arrange for the BT Equipment to be returned to BT.

- 19.2** On termination of the Service, BT will:
- 19.2.1** terminate Customer's access to the Portal(s), the Service Software and cease to provide all other elements of the Service;
  - 19.2.2** ensure the Supplier will delete the Customer transaction logs set out in Paragraph 10, in accordance with the following timescales, unless an additional time period was agreed on the Order:
    - (a)** after 30 days for operational logs,
    - (b)** audit and alert logs depending on the selected Graded Service Tier; being:
      - (i)** after 60 days for Foundation;
      - (ii)** after 120 days for Foundation Plus; and
      - (iii)** after 13 months for Premium;
  - 19.2.3** where permitted under applicable mandatory law, delete any other Content, including any configuration data relating to BT's management of the Service. Except if otherwise agreed by an Order this will be done fifteen Business Days after termination of the Service.

## Section E Service Levels and Service Credits

### 20. INTRODUCTION

- 20.1** BT will use its reasonable endeavours to achieve the service levels ("Service Levels") applicable to the Service. If BT fails to achieve the Service Levels, the Customer may claim associated service credits ("**Service Credits**").
- 20.2** Service Levels only apply to events occurring within the Service Management Boundary.
- 20.3** Service Credit calculations and payments will be based on monthly recurring Site Charges.

### 21. ON TIME DELIVERY SERVICE LEVEL

- 21.1** BT will deliver the Service on or before the Customer Committed Date ("**On Time Delivery Service Level**").
- 21.2** On Time Delivery Service Credits
  - 21.2.1** In the event that BT does not meet the On Time Delivery Service Level, the Customer may claim a service credit associated with that On Time Delivery Service Level which will be capped at 4 per cent of the monthly recurring Charge for the affected Site (an "On Time Delivery Service Credit") for each Business Day exceeding the Customer Committed date until the Operational Service Date occurs.
  - 21.2.2** If both BT and Customer have agreed a revised Customer Committed Date in writing, or if BT exercises its right to revise the Customer Committed Date on account of a change requested by Customer, the Calculation of any On Time Delivery Service Credits will be made by reference to the revised Customer Committed Date.
  - 21.2.3** Exceptions to On-Time Delivery Service Level:
    - (a)** The On-Time Delivery Service Level does not apply to upgrades or changes to the Service, unless the upgrades or changes each have an agreed delivery date, in which case the Customer Committed Date will be the same as the agreed delivery date for such upgrades or changes.
    - (b)** BT may expedite delivery of the Service for operational reasons or in response to a request from Customer, however this will not cause the original Customer Committed Date to be revised.

### 22. SERVICE AVAILABILITY SERVICE LEVEL



- 22.1 BT will assign a Service Level category for each Site ("**Site Service Level Category**") included in the Order that is determined by the Service configuration and the technical specification at that Site. Category A will apply for High Availability Sites and Category D for any non-resilient Sites. The associated service availability metrics are set out in the table below.
- 22.2 Each Site Service Level Category has an Annual Service Availability Target, a Maximum Annual Service Downtime and a Monthly Standard Service Credit Start Point which are used to ascertain when Service Credits are payable. BT will measure Service Downtime for each Qualifying Incident and will keep a record of cumulative Service Downtime by Site, in units of full minutes, for each month and a rolling 12-month period.
- 22.3 Service Downtime is measured from when a Qualifying Incident is opened on BT's incident management system and ends when BT resolves the Qualifying Incident ("Service Downtime"). The Customer will be given an Incident ticket number for each Qualifying Incident. BT will inform the Customer when the Qualifying Incident is resolved and will close the Incident ticket when either the Customer confirms within 20 minutes that the Qualifying Incident is resolved, or BT has attempted and failed to contact the Customer and the Customer does not respond within 20 minutes. If the Customer confirms that the Qualifying Incident is not resolved within 20 minutes of being informed, the Incident ticket will remain open, and the Service Downtime calculation will be adjusted.
- 22.4 Service Downtime will be suspended outside Business Hours, unless otherwise specified in the Order.

Site Service Level Category	Annual Service Availability Target	Maximum Annual Service Downtime	Monthly Standard Service Credit Start Point	Service Credit Interval	Standard Service Credits for each started Service Credit Interval	Elevated Service Credits
Cat A	≥ 99.95%	4 hours	0 minutes	Per started hour	4% of MRC	8% of MRC
Cat D	≥ 99.80%	17 hours	5 hours	Per started hour	4% of MRC	4% of MRC

22.5 Service Availability Service Credits.

22.5.1 When there is a Qualifying Incident(s) and the cumulative Service Downtime in a month at a Site exceeds the Monthly Standard Service Credit Start Point but does not exceed the Maximum Annual Service Downtime, the Customer may claim standard Service Credits. Service Credits will be four (4) per cent of the Monthly Recurring Charges ("**MRC**") for the impacted Service, per started Service Credit Interval above the Monthly Standard Service Credit Start Point.

By way of a worked example: at a Cat D Site, a Qualifying Incident with a Service Downtime of 6 hours and 10 minutes would incur 2x4% of the MRC for the impacted Service (two started Service Credit Intervals above the 5-hour Monthly Service Credit Start Point).

22.5.2 Elevated Service Credits shall apply if the cumulative Service Downtime at a Site in any rolling 12-month period exceeds the Maximum Annual Service Downtime. Elevated Service Credits shall apply to the entire Service Downtime of the Incident which triggered the breach of the Maximum Annual Downtime. The Customer may claim for each started Service Credit Interval at the percentage of MRC for the Service shown in the table above. Elevated Service Credits will remain for any further periods of Service Downtime until the Maximum Annual Service Downtime in a rolling 12-month period is no longer exceeded. Whilst Elevated Service Credits apply, Standard Service Credits and the Standard Service Credit Start Point will not apply.

By way of a worked example: at a Cat D Site, a Qualifying Incident with a Service Downtime of 8 hours in May, then a further Qualifying Incident with a Service Downtime of 10 hours in September, the Service Downtime in September would result in a breach of the Maximum Annual Service Downtime target of 17 hours. Elevated Service Credits will apply at a rate of 10x4% of the MRC for the impacted Service in September. The Elevated Service Credits shall apply if there are any additional periods of Service Downtime until the 17 hour Maximum Annual Service Downtime is no longer breached in a rolling 12-month period. Assuming there are no further Qualifying Incidents, this would be May of the following year.

## 23. GENERAL SERVICE CREDIT EXCLUSIONS

**23.1** Only measurements carried out by BT will be used in the calculation of Service Credits.

### 23.2 Service Levels and/or Service Downtime will be excluded:

- 23.2.1** where the acts or omissions of the Customer or any third party (excluding BT's suppliers) which lead to BT not being able to provide all or part of this Service; e.g. the Customer does not provide access, delays providing access or denies permission for BT or its agents and third parties, acting on BT's behalf, to implement the Service or carry out necessary repairs to the Service;
- 23.2.2** if a third party Access Line is not connected or functioning, a fault on the Customer's network, the Customer's Equipment (including configuration) or on any third-party software or service not provided and/or managed by BT under the terms of this Schedule;
- 23.2.3** for any faults caused by the Customer's use or management of the Service;
- 23.2.4** if BT is awaiting information from the Customer or awaiting confirmation by the Customer that the Service has been restored;
- 23.2.5** for any Qualifying Incident not reported in accordance with the incident reporting procedures notified by BT to the Customer or where Priority 1 Incident tickets are opened erroneously;
- 23.2.6** for any cause beyond BT's reasonable control as set out in the Governing Agreement or this Schedule;
- 23.2.7** during any period of Planned Maintenance or agreed changes on the Service by BT unless the service outage time exceeds the time estimation communicated to the Customer;
- 23.2.8** during any period of maintenance by the Customer or its third party on Customer equipment, third party software or third party services not provided and/or managed by BT under the terms of this Schedule;
- 23.2.9** during any trial period of the Service; and
- 23.2.10** if the Service is suspended due to Customer's breach of its obligations under the Governing Agreement and this Schedule.

### 23.3 General Service Credit Limitations

- 23.3.1** Service Credits for all Service Levels will be aggregated and cannot exceed 100% of the cumulative monthly recurring Charges at any affected Site.
- 23.3.2** To qualify for Service Credits, and before any Service Credits can be applied, the Customer must make a claim within 25 calendar days after the end of the month in which the Service underperformed or where a longer time period is required by mandatory local law then the shortest period that can be applied.
- 23.3.3** Service Credits will be :
  - (a)** paid by deduction from the Customer's invoice within two billing cycles of a claim being received; or
  - (b)** if related to On-Time Service Delivery Credits, paid by deduction from the first invoice following the Operational Service Date; or
  - (c)** following termination of the Service where no further invoices are due to be issued by BT, paid by BT within two months of a claim being received.

**Section F Data Protection**

This section supplements the data provisions that may be set out in the Governing Agreement:

**24. DURATION OF THE PROCESSING OF PERSONAL DATA**

**24.1** BT will Process the Customer Personal Data for the Service for as long as BT provides the Service and for as long as BT may be required to Process the Customer Personal Data in accordance with Applicable Laws.

**25. THE NATURE AND PURPOSE OF THE PROCESSING OF PERSONAL DATA**

**25.1** The nature and purpose of the Processing of Customer Personal Data by BT is the following:

- 25.1.1** provisioning of the Service by BT allowing the Customer to configure the Service implementing rules by which source and destination IP Addresses, protocols, Users and applications can be controlled via the CSP;
- 25.1.2** monitoring traffic traversing the Service to enforce the rules and CSPs implemented on the Security Appliance;
- 25.1.3** sharing Customer Personal Data with the suppliers of BT Equipment or Customer Equipment or sub-contractors as may be necessary for the provision and management of the Service including installation, maintenance and resolution of Incidents;
- 25.1.4** if the Customer have selected the Threat Emulation Service, Customer Personal Data being sent automatically from Security Appliances or Software to cloud-based infrastructure operated by the supplier for threat emulation and assessment;
- 25.1.5** accessing a log of customer IP Addresses, MAC addresses and Users, together with attempted URL and website visits by those addresses and Users, using an online Portal in order to provide the reports.

**25.2** For the provision and management of the Service parts provided by the Supplier:

- 25.2.1** depending on the respective Supplier selected; any Processing of Personal Data by the Supplier where applicable, will be subject to the Supplier's privacy policy as set out on:
  - (a)** Fortinet : <https://www.fortinet.com/corporate/about-us/privacy>. Fortinet's compliancy with regard to GDPR can be found at: <https://www.fortinet.com/corporate/about-us/gdpr>
  - (b)** Palo Alto: <https://www.paloaltonetworks.com/legal-notice/privacy>. Palo Alto's DPA can be found at: [https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/legal/palo\\_alto\\_networks\\_customer\\_data\\_processing\\_addendum.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo_alto_networks_customer_data_processing_addendum.pdf)
  - (c)** Cisco: [https://www.cisco.com/c/en\\_uk/about/trust-center/global-privacy-policy.html](https://www.cisco.com/c/en_uk/about/trust-center/global-privacy-policy.html). Cisco's DPA can be found at: <https://www.cisco.com/site/us/en/about/trust-center/data-protection-agreement.html#tabs-35d568e0ff-item-194f491212-tab>
  - (d)** Check Point: <https://www.checkpoint.com/privacy/> . Check Point's DPA can be found at: <https://www.checkpoint.com/customersdpa/>

**26. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS**

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

**26.2** The nature and purpose of the Processing of Customer Personal Data by BT includes:

- 26.2.1** name;
- 26.2.2** address;
- 26.2.3** telephone number;
- 26.2.4** email address;

- 26.2.5 job title;
- 26.2.6 company name;
- 26.2.7 contact records;
- 26.2.8 website or IP Address of destination;
- 26.2.9 IP Address of source device;
- 26.2.10 MAC (media access control) address of source device;
- 26.2.11 transaction logs, and
- 26.2.12 identity management - user profiles.

This list is not exhaustive as the Customer will specify what Customer Personal Data is Processed.

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

- 26.3.1 Customer's end users; and
- 26.3.2 Customer's employees, directors and contractors and other third parties of the Customer; and
- 26.3.3 Any Data Subject controlled by the Customer

This list is not exhaustive as the Customer will specify any other categories of Data Subjects.

## Section G 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 C.

“**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.

“**Administrator**” means the person(s) authorised by the Customer who is responsible for managing the Service using the Portal(s).

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

“**Botnet**” is a group of interconnected devices, each of which runs more bots. Botnets can be used to perform distributed denial-of-service attacks. Steal data, send Spam, allowing the attacker to access the device and its connection.

“**BT Network**” means the communications network of BT.

“**BT Portal**” means the online user interfaces used by BT and the Customer to manage the Service in-life, as set out in Part B.

“**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 fees and charges payable by the Customer in relation to a Service as set out in the Order.

“**Co-Management**” allows a level of control by BT and the customer by allowing the customer to self serve the SSR (simple service request)

“**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 Security Appliances and determine the operation of the Service.



“**Customer Handbook**” means a document provided to the Customer upon completion of the first Order to provide information relevant to the Graded Service Tier and Service Options purchased. The Customer Handbook is not a contractual document.

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

“**Customer Transaction Logs**” means, the metadata of all network traffic sent to or received by the Supplier from or to the Customer in the Customer's use of the Service.

“**CVSS**” means Common Vulnerability Scoring System v4.0; a public framework for rating the severity and characteristics of security vulnerabilities in information systems. It provides a numerical score ranging from 0 to 10 to indicate the severity of a vulnerability, with 10 being the most severe. A “**High CVSS Score**” means a CVSS score range from 7.0 to 8.9 and a “**Critical CVSS Score**” means a CVSS score range from 9.0 to 10.0.

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

“**DNS Transaction**” means a recursive DNS query sent from the Customer through its use of the Service.

“**Domain Name Service**” or “**DNS**” means a directory system which translates numeric IP Addresses into domain names to identify Users on the Internet.

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

“**Foundation**” means the Foundation Graded Service Tier as set out in Part B.

“**Foundation Plus**” means the Foundation Plus Graded Service Tier as set out in Part B.

“**Graded Service Tier**” is the term used to describe the level of management features for the Service and is classified as either Foundation, Foundation Plus or Premium.

“**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.

“**High Availability Site**” means a Customer's Sites having dual Security Appliances with failover as set forth in the Order.

“**Hyper-Text Transfer Protocol**” or “**HTTP**” means an application protocol for distributed, collaborative, hypermedia information systems.

“**Hyper-Text Transfer Protocol Secure**” or “**HTTPS**” means a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

“**Indicators of Compromise**” or “**IOCs**” are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.

“**Incident**” means either a Technical or a Security Incident.

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

“**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.

“**Known Virus**” means a virus that, at the time of receipt of content by the Supplier, a signature has already been made publicly available, for a minimum of one hour for configuration by the Supplier's third party commercial scanner.

“**Malware**” is short for malicious software specifically designed to disrupt, damage or gain unauthorized access to a computer system.

“**Mitigation Action**” means a recommended mitigating action which should be taken to address the impact of IOCs identified by BT.



“**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 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.

“**Premium**” means the Premium Graded Service Tier as set out in Part B.

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

“**RBAC Profile**” means the Role Based Account Control Profile provided as part of the Co-Management Service Option.

“**Security Appliance**” means any firewall equipment, being either BT Equipment or Customer Equipment.

“**Security Incident**” means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempt underway) exploitation of an existing Vulnerability, and that has a significant probability of compromising business operations and threatening information security.

“**Service Desk**” means the helpdesk that the Customer is able to contact to submit service requests, report Incidents and ask questions about the Service 24 hours a day; 365 days per year.

“**Session**” means any non-HTTP or HTTP request sent to or from the Customer through its use of the Service.

“**Security Support**” means the BT person which provides support to the Customer for any in-life service management aspects as set out in Part B. This can be either a security optimisation manager and/or a service relationship manager and/or a threat analytical manager depending on the particular support aspect.

“**Spam**” means unsolicited usually commercial messages (such as emails, text messages, or Internet postings) sent to a large number of recipients or posted in a large number of places.

“**SSR**” or “**Simple service request**” means Simple Service Request as set out in Part B.

“**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” or “Minimum Term”.

“**Supplier**” means depending on which firewall supplier being selected on the Order; a) Fortinet Inc., 899 Kiffer Road, Sunnyvale, California 94086, United States of America, b) Cisco International Limited having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, TW14 8HA, UK and any group or parent company of the Supplier, c) Palo Alto Networks Inc. whose registered office is at 4401 Great America Parkway, Santa Clara, California, 95054, USA or Palo Alto Networks (Netherlands) B.V. whose registered office is at Oval Tower, 5<sup>th</sup> Floor, De Entrée 99-197, 1101HE Amsterdam, the Netherlands or d) Check Point Software Technologies Ltd. 5 Shlomo Kaplan Street Tel Aviv 6789159, Israel.

“**Supplier Software**” means Supplier Software for use during the licence period as set out in the Order to download and install on the Security Appliances. This software enables the Customer to use the Service.

“**Technical Incident**” means either any unplanned interruption to, or a reduction in the quality of, the Service or a Service component.

“**Uniform Resource Locator**” or “**URL**” means a character string that points to a resource on an intranet or the Internet.

“**Unknown Viruses**” means any virus that has not being identified yet as Known Virus.

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

“**Vulnerability**” means a software susceptibility that may be exploited by an attacker.