BT Managed Cloud Security (Prisma Access) Service Schedule Part A – Service Terms

Section A Service Terms

1. SERVICE SUMMARY

1.1 BT's Managed Cloud Security (Prisma Access) provides the Customer with Supplier Software that protects the Customer and its Users. Protection includes threats from Known Viruses from the Internet, improved prevention against Unknown Viruses using the Sandbox technology, secure access to applications and managing User experience, based on various subscription functions and features available as set out in any applicable Order, comprising:

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.

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 seven (7) calendar days in advance when it concerns BT Planned Maintenance. Any planned maintenance by the Supplier shall be carried out in accordance with the timeframes set out by the Supplier at https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/upgrade-types.

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

2.2.3 node reconfiguration due to refresh programs by the Supplier.

2.3 BT may occasionally suspend the Service in an event of 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 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 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 perform its obligations here under with respect to the Service, e.g. providing the Customer Security Policy and application details to be implemented on the Service;

3.1.3 undertake the setting up any User groups that may be required on the Customer's authentication server which the Customer will reflect in the Customer Security Policy. The Customer will do this using the Portal(s);

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 that the Enabling Service is working correctly before reporting any 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 the Customer's firewall configurations and network settings allow the traffic types necessary for BT to provide the Service;

3.1.15 use one of the methods supported by the Supplier to authenticate Users, which are set out at https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-api/get-started-with-saas-security-api/manage-saas-security-api-administrators/select-an-authentication-method(or any other online address that BT may advise);

3.1.16 where applicable, be responsible for deployment of the Global Protect Client on Users' Devices and the configuration and management of all settings relevant to mobile users and Remote Networks;

3.1.17 be responsible for downloading and deploying the Supplier Software to User Devices.

3.1.18 use best endeavours to remediate any problems encountered during the process of deploying the Supplier Software to User Devices;

3.1.19 provide consent to;

(a) BT and the Supplier to use, reproduce, store, modify, and display the information from the Customer Transaction Logs for the purpose of providing the Service;

(b) BT and the Supplier to use the Threat Logs related to the Service for the purpose of: (i) maintaining and improving the Service; (ii) complying with all legal or contractual requirements; (iii) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service; (iv) anonymously aggregating and statistically analysing the content; and (v) other uses related to the analysis of the Service;

(c) BT and the Supplier 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 Customer's confidential information;

(d) BT and the Supplier to apply signature updates automatically;

(e) BT and Supplier personnel to provision the Service within the multitenant Portal set up for the Customer for the purposes of providing the managed service, e.g. maintenance, troubleshooting, implementing service requests, service management, etc. and

(f) BT to maintain administrator credentials or privileged account where required for configuring applications.

3.1.20 be responsible for establishing communication between the Customer's internal helpdesk and its Users;

3.1.21 be responsible to maintain back-up configurations to allow all the associated services to be restored to a previous state in the event of any misconfiguration that may result in the service being compromised or inoperable;

3.1.22 except if otherwise agreed on the Order; be responsible for implementing any Mitigation Action using the Portal(s); and

3.1.23 If the Customer orders Co-Management option as set out in Part B, be responsible for:

(a) ensuring that the Customer's authorised nominated Users complete the 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.

3.1.24 If the Customer orders the Co-operative Mitigation option with Premium Graded Service, the Customer will:

(a) indicate in the Order the appropriate specific endpoint Devices or End-User Identities are excluded for which BT is not authorised to take any Mitigation Action in relation to specific security controls;

(b) select in the Order whether BT's authority at Paragraph 3.1.24(a) is done either automatically or subject to the Customer's approval; and

(c) securely provide BT with the necessary access credentials to the platforms that are used by the Customer to make policy changes to the endpoints or End-User Identities requiring Co-operative Mitigation and notify BT of any subsequent changes to these credentials.

3.2 As the Customer is deemed to have approved all changes to the Customer Security Policy and or configuration changes 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. CUSTOMER EQUIPMENT

4.1 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;

4.1.2 monitor and maintain any Customer Devices used in connection with the Service;

4.1.3 ensure that any Customer Devices that the Customer uses, directly or indirectly, in relation to the Service:

(a) is technically compatible with the Service; and

(b) is approved and used in accordance with relevant instructions, standards and Applicable Law, license terms and any safety and security procedures applicable to the use of that Customer equipment.

4.2 The Customer agrees that BT will not be liable for any failure by the Customer to comply with this Paragraph 4 and the Customer will be liable to BT for any claims, losses, costs or liabilities incurred or suffered by BT due to the Customer's failure to comply with this Paragraph 4.

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, BT may restrict or suspend the entire Service upon notice; e.g. by blocking source IP Addresses or suspend Customer's access to the Service. In such event:

5.2.1 the Customer will continue to pay the Charges for the Service until the end of the Subscription Term; and

5.2.2 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 for this also execute a power of attorney as part of the Order.

6. PASSWORDS, AUTHORISED USERS AND SECURITY

6.1 Obligations applicable to any User.

6.1.1 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) distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Service;

(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.

(g) agree to pay for any usage above the volume or capacity purchased

6.2 Obligations applicable to Administrator(s).

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

(a) not remove or alter the Administrator account without BT's prior consent;

(b) avoid unauthorised access to the Administrator account;

(c) 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;

(d) 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 configuration;

(e) 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;

(f) keep personnel access to the Administrator account up to date; and

(g) keep records of any changes and make these available to BT where required.

6.3 If the Customer fails to comply with Paragraph 6, BT reserves the right to remove the Customer's administration rights.

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 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.

7.2 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.

7.3 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.

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.

8. CUSTOMER TRANSACTION LOGS

8.1 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.

8.2 BT and the Supplier may, use the Malware, Spam, Botnets or other information related to the Service for the purpose of:

8.2.1 maintaining and improving the Service;

8.2.2 complying with all legal or contractual requirements;

8.2.3 making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service;

8.2.4 anonymously aggregating and statistically analysing the content;

8.2.5 other uses related to the analysis of the Service;

8.2.6 Compiling reports for customer consumptions; and

8.2.7 Other Value add service such as ticketing systems.

8.3 BT will use reasonable endeavours to transmit and store the logs securely. Logs will be stored in their raw state or compressed if appropriate.

8.4 The Customer will confirm its specific logging requirements at the time of placing the Order. For any Customer specific requirements that BT deems are non-standard, an additional Charge shall be agreed on the Order.

8.5 If requested by the Customer and subject to an additional Charge as agreed on an Order, logs may be sent to and stored in a repository on the Customer Site or third-party premises based on a design that is agreed and:

8.5.1 BT will not be responsible for the logs while they are sent to or stored in such a repository;

8.5.2 paragraphs 8.3 and 8.4 will not apply to logs sent to or stored in such a repository;

8.5.3 the Customer will take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with BT; and

8.5.4 the Customer will ensure that the Customer or the nominated third party use reasonable endeavours to secure the repository appropriately.

9. SUGGESTIONS, IDEAS AND FEEDBACK

9.1 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

10. INTRODUCTION

10.1 The Customer acknowledges they have read and agree to be bound by and to ensure that any Users will comply with this Section B ("**Acceptable Use Policy**" or "**AUP**") and the Supplier's acceptable use policy as set out at: https://www.paloaltonetworks.com/legal-notices/terms-of-use. Where the Customer selects the Palo Alto Networks Wildfire Service option the Customer will comply with the following AUP: https://www.paloaltonetworks.co.uk/resources/datasheets/wildfire-acceptable-use-policy

11. USE OF THE SERVICE

11.1 The Customer will not use the Service in breach of Applicable Law or in any way that is considered to be:

11.1.1 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

11.1.2 detrimental to the provision of services to the Customer or any other BT customer.

11.2 The Customer will not use the Service to intentionally take, or attempt to take, any action that could:

11.2.1 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

11.2.2 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.

12. USE OF MATERIALS

12.1 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:

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

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

12.1.3 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;

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

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

12.2 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.

13. SYSTEMS AND SECURITY

13.1 The Customer will not:

13.1.1 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.

13.1.2 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;

13.1.3 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

13.1.4 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

14. EXPORT OF CONTENT USING CLOUD SERVICES

14.1 The Service comprises of a cloud service that uses 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.

15. PCI DSS

15.1 The Service is not compliant with PCI DSS nor is it designed nor intended to be and the Customer will not use the Service for the processing, storage or transmission of any cardholder data or and data that is subject to PCI DSS.

15.2 The Customer will be responsible for ensuring that the Service does not affect the security of any other service they have that contain data that is subject to PCI DSS.

15.3 The Customer will indemnify BT from any claims, costs or liabilities that it incurs as a result of the Customer storing processing or transmitting data that is subject to PCI DSS.

Section D Charges, Subscription Term and Termination

16. CHARGES

16.1 The Customer will pay the Charges for the Service and any optional features (including upgrades and re-configuration) as specified in the Order.

16.2 In addition to the Charges set out in the Order, the Customer may be liable for the following additional Charges:

16.2.1 Charges for (de-)commissioning the Service outside of Business Hours;

16.2.2 Charges for expediting provision of the Service at Customer's request after BT has informed Customer of the delivery date;

16.2.3 Charges for investigating Customer reported Incidents where BT finds no Incident or that the Incident is outside the Service Management Boundary;

16.2.4 Charges for restoring Service if the Service has been suspended by BT in accordance with the terms of the Governing Agreement;

16.2.5 Charges per element re-configured after the Operational Service Date must be agreed and documented in a new Order;

16.2.6 Charges for additional SSRs that exceed those included with the Service; and

16.2.7 Charges for Complex Changes.

16.3 The Customer acknowledges and agrees to be bound by and to ensure that any Users will comply with the Supplier Licensing and Fair Use policy as set out at https://www.paloaltonetworks.com/legal-notices/terms-of-use. This includes participating in any reviews requested by BT and or the Supplier in relation to over usage and agreeing to take corrective action, which may include increasing subscription/s and or payment for over usage that has already happened. BT shall ensure that the Supplier will provide the over usage details.

16.4 If BT can evidence that the number of Users in any month exceeds the numbers ordered by the Customer, the Customer shall within the timescales set out in BT's notification either:

16.4.1 decrease the number of Users; or

16.4.2 agree by a new Order the increased number of User and the applicable Charges.

17. SUBSCRIPTION TERM, TERMINATION AND RENEWAL

17.1 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.

17.2 Unless the Parties agree to renew the Subscription Term by Order, following the expiry of any Subscription Term the Service shall terminate at midnight on the last day of the Subscription Term.

17.3 The Customer may request for a renewal in writing to BT at least 90 days before the end of the Subscription Term or subsequent renewal period specifying the new required renewal period. BT will provide one of following responses to the Customer:

17.3.1 BT may issue a draft Order to the Customer on the existing terms and/or Charges for the renewal period; or

17.3.2 BT may issue a draft Order to the Customer on amended terms for the renewal period; or

17.3.3 where renewal of the Service is not possible BT will provide an explanation why.

18. END OF SERVICE

18.1 On termination of the Service, the Customer will:

18.1.1 retrieve all Customer data from the Service;

18.1.2 provide BT with all assistance necessary to remotely decommission all applications supporting the Service;

18.1.3 remove all Software associated with the Service for Customer's Devices used in connection with the Service.

18.2 On termination of the Service, BT will:

18.2.1 terminate Customer's access to the Portal(s), the Service Software and cease to provide all other elements of the Service; and

18.2.2 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

19. SUPPLIER SERVICE LEVELS AND CREDITS

19.1 The Customer may claim directly from the Supplier service credits for the Supplier service levels as set out at https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/prisma-access-service-sla.pdf.

19.2 In order to submit a claim for Service Credits the Customer is required to:

19.2.1 Open a case on the Portal within 24 hours of an Incident; and

19.2.2 Submit a claim on the claim dashboard within five (5) business days of the Incident.

19.3 Once the Supplier confirms to the Customer and BT that the claim is accepted, BT will pay the service credits awarded by the Supplier:

19.3.1 by deduction from the Customer's invoice within two (2) billing cycles of a claim and service credits being confirmed by the Supplier; or

19.3.2 following termination of the Service where no further invoices are due to be issued by BT, within two months of a claim and service credits being confirmed by the Supplier.

There are no other Service levels with Service credits available for this Service, only Service targets as set out in part B.

Section F Data Protection

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

20. DURATION OF THE PROCESSING OF PERSONAL DATA

20.1 BT or its Sub-Processor 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.

21. THE NATURE AND PURPOSE OF THE PROCESSING OF PERSONAL DATA

21.1 The nature and purpose of the Processing of Customer Personal Data by BT and the Supplier is as follows:

21.1.1 the Service allows the Customer to set rules by which network traffic, users, files, access to applications or domains could be blocked by the security controls applied as defined in the Customer Security Policy

21.1.2 if the Customer requests a management and monitoring overlay, and/or Eagle-I, BT will set up log forwarding from the Supplier logging service to a BT SIEM (Only applicable for Foundation plus and Premium GSM levels). These will be sent to 2 destinations:

(a) BT's Internal logging platform within BT's UK datacentres. This data is used for security and health-based monitoring. Additionally, this will be used to build reports for customers as part of their Service.

(b) Eagle-i – to deliver a proactive security service for the Customer. If BT is reselling the Service to the Customer, then BT will neither be a Controller or a Processor of Personal Data.

21.1.3 any Processing of Personal Data by the Supplier where applicable, will be subject to the Supplier's privacy policy as set out on https://www.paloaltonetworks.com/legal-notices/trust-center.

22. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

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

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

22.2.1 website or IP address (for network devices and relating to an individual's device) or media access control (MAC) address;

22.2.2 name;

22.2.3 address;

22.2.4 telephone number;

22.2.5 email address;

22.2.6 job title;

22.2.7 company name;

22.2.8 contact records;

22.2.9 usage records (call, internet or router logs);

22.2.10 transaction logs;

22.2.11 identity management - user profiles;

22.2.12 account details.

22.2.13 support/ service records;

22.2.14 general company name/ employer general location data identifiers;

22.2.15 service/product data content of communications (from network) Inferences drawn from Service/ product data network location data; and

22.2.16 preferences/ setting configurations Service/ products analytics system logs device location data network weblogs Usage data.

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

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

22.3.1 Customer's end users; and

22.3.2 Customer's employees, directors and contractors and other third parties of the Customer; and

22.3.3 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.

"**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.

"**Customer Handbook**" means a 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.

"**CSP**" or "**Customer Security Policy**" means the Customer's security policy containing the security rules, set and owned by the Customer, that are applied to the Software and determine the operation of the Service.

"**Customer Transaction Logs**" means, the metadata of all network traffic and Security events sent to or received by the Supplier from or to the Customer during the Customer's use of the Service.

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

"Digital Experience Monitoring" or "**DEM**" is a technology monitoring the availability, performance and quality of an User experience when using a cloud, software as a service or web application.

"**Device**" means any equipment, including but not limited to laptops and servers, used by the Customer or Customer's employees to provide or gain an access to Customer's applications, systems and platforms.

"**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.

"**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.

"**Location**" means a specific access point to the Internet in connection with the Service.

"**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.

"**PCI DSS**" means the Payment Card Industry Data Security Standards, a set of policies and procedures, issued by the PCI Security Standards Council LLC (as may be adopted by local regulators) and intended to optimise the security of credit and debit card transactions and protect cardholders against misuse of their personal.

"**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.

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

"**Remote Networks**" means a virtual private network that enable Users who are working at branch sites to connect to the corporate data centre, encrypting all traffic the Users send and receive.

"**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.

"**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**".

"**Supplier**" means either 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, 5th Floor, De Entrée 99-197, 1101HE Amsterdam, the Netherlands.

"**Supplier Software**" means Supplier Software for use during the licence period as set out in the Order for the Customer to download and install on User devices. This software enables the Customer to use the Service.

"**Supplier Platform**" means the software as a service platform, provided by the Supplier and managed by BT, that provides the core technical capabilities allowing the Customer to secure and manage their assets, applications and Users.

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

"**Threat Log**" - means system generated logs that tracks alert events when traffic matches one of the security profiles. Each entry includes information such as; the date and time, type of threat, threat description, source and destination zones, addresses, ports, action (such as allow or block) and severity level.

"**Transaction**" means an HTTP or HTTPS request sent to or from the Customer through its use of the Service.

"**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.