BT Compute Protect
Annex to BT Cloud Environment Services

1 Definitions

The following definitions apply, in addition to those in the General Terms and Conditions and the related BT Cloud Environment Service(s). In the case of conflict between these defined terms and the other defined terms, these defined terms will take precedence for the purposes of this Schedule.

"**BT Cloud Environment Service**" means a BT-branded service or product through which BT offers or markets to its customers a BT cloud environment for their own business use; being BT Cloud Compute, BT Compute for Microsoft® Azure services, BT Private Compute or any other service BT may later make available for which BT Compute Protect can be selected with.

"Compute Protect" means the Service as set out in Clause 2 below.

"Deep Packet Inspection" means a form of computer network packet filtering that examines the data part of a packet as it passes an inspection point, searching for security issues such as protocol non-compliance, viruses, spam and intrusions.

"Security Modules" means the security modules as set out in Clause 3.1 below.

"Stateful Firewall" means a firewall that keeps track of the state of network connections travelling across it. It allows the Customer to restrict access to the VM only to the necessary ports, protocols and IP addresses for the correct functioning of the server and application, reducing the risk of unauthorised access.

"**Supplier**" means Trend Micro (UK) Limited, with company number 03698292 having its principal place of business at Podium Level, 2 Kingdom Street, London, W2 6BD.

"Virus Pattern Files" means a computer file used to help capture viruses, often working in tandem with a larger antivirus program.

2 Service Summary

2.1 Compute Protect Service is an optional value added security service that provides the Customer with a right to access and use a self-service portal where the Customer can select and configure modules to protect Virtual Machines against Internet security threats, comprising the Standard Service Components up to the Service Management Boundary as set out in this Annex.

2.2 In order to use the Compute Protect Service, the Customer will have in place or will purchase the following services that will connect to the Compute Protect Service and are necessary for the Compute Protect Service to function and will ensure that these services meet the minimum technical requirements as agreed with BT:

(a) a BT Cloud Environment Service; and

(b) an Internet connection.

2.3 Compute Protect Service is provided on a pay as you go basis. Ordering, termination and invoicing shall be subject to the terms as agreed for the related BT Cloud Environment Services.

3 Standard Service Components

BT will provide the Customer with all the following standard service components in accordance with the details as set out in any applicable Online Order:

3.1 **Security Modules:** The Customer will be able to choose and configure via the Portal any of the following standard security modules provided by the Supplier:

3.1.1 **Anti-malware:** protects VMs against viruses and other malware;

3.1.2 **Web reputation service:** protects Users and applications by blocking access to malicious URLs;

3.1.3 **File and system integrity monitoring for compliance:** helps to detect unauthorised, unexpected and suspicious changes to files, directories, registry keys and values;

3.1.4 **Intrusion detection and protection:** enables Deep Packet Inspection to provide protection against the exploitation of network security vulnerabilities;

3.1.5 **Stateful Firewall:** allows the Customer to restrict access to the VM only to the necessary ports, protocols and IP addresses for the correct functioning of the server and application, reducing the risk of unauthorised access; and

3.1.6 **Log inspection:** enables the Customer to identify and report important security events.

3.2 **Information and Reports:** BT will provide the Customer, via the Portal, with access to security monitoring information and reports depending on the modules that the Customer has selected in the Order.

3.3 **Updates:** BT will provide the Customer, via the Portal, with continuous and automatic updating of Virus Pattern Files to protect against Internet security threats.

4 BT Obligations and Service Management Boundary

In addition to any other BT obligations as set out in the Agreement;

4.1 BT's Service Management Boundary is limited to provide and manage the combination of above described Security Modules the Customer has chosen in any Online Order.

4.2 BT will have no responsibility for the Service outside the Service Management Boundary; more in particular:

(a) BT does not make any representations, whether express or implied, about whether the Compute Protect Service will operate in combination with any Customer Equipment or other equipment and software.

(b) given the nature and volume of malicious and unwanted electronic content, BT does not warrant that the Compute Protect Service is error free or will detect all security or malicious code threats or that use of the Compute Protect Service will keep the Customer's Network or computer systems free from all viruses or other malicious or unwanted content or safe from intrusions or other security breaches. Therefore BT's liability – as far as allowed under applicable law – is limited to put in place the appropriate diligence and means to detect and/or mitigate viruses, unwanted content, intrusions, malicious code or other security threats as set out in this Annex; without any commitment on the results. BT may however directly or through its Supplier, take reasonable steps to prevent any unauthorised access.

4.3 The Compute Protect Service is neither designed nor intended for use in:

(a) the design, construction, operation or maintenance of any nuclear facility;

(b) aircraft navigation, communications, or operating systems;

(c) air traffic control systems;

(d) operating life-support or life critical medical equipment; or

(e) any other equipment or systems in which the circumvention or failure of Compute Protect Service could lead or contribute to death, personal injury, or physical property or environmental damage.

4.4 BT disclaims and excludes any rights set out in the licence terms, as well as any express or implied warranty of fitness, for such uses.

4.5 BT's Supplier may:

(a) use uploaded data from the embedded software to improve its products and services;

(b) share data that has been identified as malicious or unwanted content with their affiliates and security partners; or

(c) use and disclose uploaded data for analysis or reporting purposes only if any such use, sharing or disclosure does not identify the Customer or include any information that can be used to identify any individual person.

5 Customer Obligations

In addition to any other Customer obligations as set out in the Agreement;

5.1 The Customer will install Agents on their VMs in order to use Compute Protect Service.

5.2 The Customer may select and configure Security Modules using the Porta, and is responsible for the correct configuration of the Security Modules

5.3 The Customer will regularly backup their data and computer systems on separate media.

5.4 The Customer will not:

(a) transfer or sub-licence the Compute Protect Service, including any embedded Software or related documentation to another person or entity;

(b) rent, lease, loan, auction, or resell the Compute Protect Service, any embedded software and related documentation;

(c) use the Compute Protect Service or any embedded software to provide services to third parties; and

(d) use the Compute Protect Service other than as specifically described in and in accordance with the accompanied documentation that comes with the Compute Protect Service or authorise others to do any of the actions set out in this Clause.

6 Additional Terms and Data Protection

6.1 The Customer acknowledges that shrink-wrap, click-wrap, or other terms and conditions or agreements ("Additional Terms") provided with the Software (and whereby the use of the Software requires an "acceptance" of those Additional Terms before access is permitted) will not be binding on BT, but only between the Supplier and the Customer. This includes any data protection conditions as set out in the Additional Terms.

6.2 BT's obligations regarding data protection are described in the respective BT Cloud Environment Service(s) purchased with BT Compute Protect.

6.3 For the avoidance of doubt, BT will process Personal Data only to the extent required for providing the Standard Service Components set out this document and BT will not have access to Personal Data and/or other confidential information that may be shared between the Customer and the Supplier regarding the use of the Compute Service. Any handling activities for using the Compute Service will be governed by the Additional Terms between the Customer and the Supplier and therefore BT will not be responsible and liable for the security and the processing of any Personal Data in connection with Customer' use of the Compute Service. Any claims and/or complaints in relation to the security and the processing of any such Personal Data may only be made by the Customer against the Supplier under the Additional Terms.