



BT Compute Protect server security Schedule to the General Terms

Contents

A note on 'you'	2
Words defined in the General Terms	2
Part A – The BT Compute Protect server security Service	2
1 Service Summary	2
2 Standard Service Components	2
3 Service Management Boundary	2
4 Associated Services and Third Parties	2
5 Specific Terms	3
Part B – Service Delivery and Management	6
6 BT's Obligations	6
7 Your Obligations	6
8 Notification of Incidents	7
Part C – Service Levels	8
9 Service Levels	8
Part D – Defined Terms	9
10 Defined Terms	9

A NOTE ON 'YOU'

'You' and 'your' mean the Customer.

WORDS DEFINED IN THE GENERAL TERMS

Words that are capitalised but have not been defined in this Schedule have the meanings given to them in the General Terms.

Part A – The BT Compute Protect server security Service

1 SERVICE SUMMARY

BT will provide you with a right to access and use a self-service portal where you 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 Paragraph 3 ("**Compute Protect server security Service**").

2 STANDARD SERVICE COMPONENTS

BT will provide you with all the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable Order:

- 2.1 **Security Modules:** You will be able to choose and configure via the Portal any of the following standard security modules provided by the Supplier ("**Security Modules**"):
 - 2.1.1 **Anti-malware:** protects VMs against viruses and other malware;
 - 2.1.2 **Web reputation service:** protects Users and applications by blocking access to malicious URLs;
 - 2.1.3 **File and system integrity monitoring for compliance:** helps to detect unauthorised, unexpected and suspicious changes to files, directories, registry keys and values;
 - 2.1.4 **Intrusion detection and protection:** enables Deep Packet Inspection to provide protection against the exploitation of network security vulnerabilities;
 - 2.1.5 **Stateful Firewall:** allows you 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
 - 2.1.6 **Log inspection:** enables you to identify and report important security events.
- 2.2 **Information and Reports:** BT will provide you, via the Portal, with access to security monitoring information and reports depending on the modules that you have selected in the Order.
- 2.3 **Updates:** BT will provide you, via the Portal, with continuous and automatic updating of Virus Pattern Files to protect against Internet security threats.

3 SERVICE MANAGEMENT BOUNDARY

- 3.1 BT will provide and manage the Service in accordance with Part B of this Schedule ("**Service Management Boundary**").
- 3.2 BT will have no responsibility for the Compute Protect server security Service outside the Service Management Boundary.
- 3.3 BT does not make any representations, whether express or implied, about whether the Compute Protect server security Service will operate in combination with any Customer Equipment or other equipment and software.
- 3.4 The Supplier will not have any direct liability to you.
- 3.5 Given the nature and volume of malicious and unwanted electronic content, BT does not warrant that the Compute Protect server security Service is error free or will detect all security or malicious code threats or that use of the Compute Protect server security Service will keep your network or computer systems free from all viruses or other malicious or unwanted content or safe from intrusions or other security breaches.

4 ASSOCIATED SERVICES AND THIRD PARTIES

- 4.1 You will have in place or will purchase the following services that will connect to the Compute Protect server security Service and are necessary for the Compute Protect server security Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:
 - 4.1.1 a BT Cloud Environment Service; and
 - 4.1.2 an Internet connection.

(each an “Enabling Service”).

- 4.2 You will provide and maintain any Customer Equipment necessary for the Enabling Services. You will pay all charges related to provision, maintenance and use of such Enabling Services and report any incidents on these Enabling Services directly to the suppliers for each Enabling Service.
- 4.3 If BT provides you with any services other than the Compute Protect server security Service (including, but not limited to any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms.

5 SPECIFIC TERMS

5.1 Changes to the Compute Protect server security Service

- 5.1.1 BT may amend the Charges at any time by either:
 - (a) publishing the amendment online via the Portal; or
 - (b) by giving Notice to you.
- 5.1.2 In relation to Paragraph 5.1.1, the Charges will be available also via the Portal on the Utility Rate Card.
- 5.1.3 BT may propose changes to this Schedule (unless those changes relate to the Charges where Paragraph 5.1 applies) by giving you Notice at least 30 days prior to the change taking effect (“Notice to Amend”).
- 5.1.4 Within 21 days of any Notice to Amend, you will provide BT Notice:
 - (a) agreeing to the changes BT proposed, in which case those changes will apply from the date of our agreement; or
 - (b) terminating the Contract.
- 5.1.5 If we have not reached agreement in accordance with Paragraph 5.1.4(a) within 15 days, the terms of this Schedule will continue to apply unless you give Notice in accordance with Paragraph 5.1.4(b) or BT may give Notice of termination, in which case BT will immediately cease delivering the Compute Protect server security Service.
- 5.1.6 Except as set out above in Paragraphs 5.1.1 and 5.1.3, both of us will agree any other changes to the Contract in accordance with the provisions in Clause 31 of the General Terms.

5.2 Termination for Convenience

- 5.2.1 The following clause will replace and supersede Clause 17 of the General Terms.
- 5.2.2 You may terminate the Compute Protect server security Service via the Portal at any time.
- 5.2.3 If you terminate the Compute Protect server security Service in accordance with Paragraph 5.2.2:
 - (a) you will pay any outstanding Charges for services rendered up to the date of termination; and
 - (b) BT will refund any remaining balance which you have paid in advance, but the refund will be subject to adjustment for any discounts that have been received due to the advance payment.
- 5.2.4 Terminating the Compute Protect server security Service in accordance with paragraph 5.2.2 above will result in the loss of any unused Monthly Allowance.
- 5.2.5 BT may, at any time after the Service Start Date and without cause, terminate the Compute Protect server security Service or any applicable Order by giving you at least 90 days’ Notice.

5.3 Licence

- 5.3.1 BT gives you the non-exclusive, non-transferable and limited right to use the Compute Protect server security Service for your internal business purposes only.
- 5.3.2 BT may directly or through the Supplier, take reasonable steps to prevent unauthorised access to, or use of, the Compute Protect server security Service.
- 5.3.3 You will not and you will not allow others to:
 - (a) try to decipher, disassemble, decrypt, discover the source code or object code or underlying ideas, algorithms, file formats, programming, or interoperability interfaces of the Compute Protect server security Service, including any embedded software;
 - (b) sell, transfer or sub-licence the Compute Protect server security Service, including any embedded software or related documentation to another person or entity;
 - (c) rent, lease, loan, auction, or resell the Compute Protect server security Service, any embedded software and related documentation;

- (d) adapt, translate or create derivative works of the Compute Protect server security Service, any embedded software or related documentation;
- (e) use Compute Protect server security Service or any embedded software to provide services to third parties; and
- (f) use the Compute Protect server security Service other than as specifically described in and in accordance with the accompanied documentation that comes with the Compute Protect server security Service or authorise others to do any of the actions set out in this Paragraph 5.3.3.

5.3.4 You grant BT and the Supplier the right to:

- (a) use uploaded data from the Compute Protect server security Service to improve their 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 you or include any information that can be used to identify any individual person.

5.3.5 **Additional Terms**

- (a) Any Additional Terms will not be binding on BT, the Supplier or you, even if use of the Compute Protect server security Service requires you to “**accept**” those Additional Terms before you are granted access to them.

5.4 **Service Limitations**

5.4.1 The Compute Protect server security 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 server security Service could lead or contribute to death, personal injury, or physical property or environmental damage.

5.4.2 You will responsible for your compliance with the Additional Terms directly to the third party supplier listed on those Additional Terms. BT will have no responsibility to you in relation to the Additional Terms.

5.5 **Invoicing**

5.5.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:

- (a) Usage Charges, monthly in arrears (depending on your billing frequency as set out in the Order), calculated at the then current hourly rates set out on the Portal;
- (b) if set out in an Order, a Monthly Allowance; and
- (c) Professional Services Charges, if applicable.

5.5.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

- (a) Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Contract;
- (b) Charges for commissioning the Compute Protect server security Service in accordance with Paragraph 6.1 outside of Business Hours;
- (c) Charges for expediting provision of the Compute Protect server security Service at your request after BT has informed you of the Service Start Date; and
- (d) any other Charges as set out in any applicable Order or the BT Price List or as otherwise agreed between both of us.

5.5.3 You may purchase the Monthly Allowance in advance at the beginning of a calendar month and BT will apply the Monthly Allowance as a credit on your account against your Usage Charges for that month. Any unused Monthly Allowance will be carried forward to the next billing period.

5.6 **Service Amendment**

- 5.6.1 You may make changes to the Security Modules you wish to use as part of the Compute Protect server security Service via the Portal at any time. It is your responsibility to ensure that any changes you make to the Security Modules have been correctly applied on the Portal.
- 5.6.2 If you make a change to the Compute Protect server security Service in accordance with Paragraph 5.6.1, the Charges you have to pay for the Compute Protect server security Service will automatically update on the Portal within two Business Days of the date you made your changes to the Compute Protect server security Service.
- 5.6.3 If BT changes the Compute Protect server security Service prior to the Service Start Date because you have given BT incomplete or inaccurate information, BT may, acting reasonably, apply additional Charges.

Part B – Service Delivery and Management

6 BT'S OBLIGATIONS

6.1 Commissioning of the Service

Before the Service Start Date, BT will:

- 6.1.1 connect the Compute Protect server security Service to each Enabling Service; and
- 6.1.2 on the date that BT has completed the activities in this Paragraph 6.1, confirm to you the Service Start Date.

6.2 During Operation

On and from the Service Start Date, BT:

- 6.2.1 will respond and use reasonable endeavours to remedy an Incident without undue delay if you report an Incident with the Compute Protect server security Service or the BT Network;
- 6.2.2 will maintain the Portal and a server to provide you with online access to performance reports;
- 6.2.3 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the BT Network, BT Equipment or the Portal, however, BT may inform you with less notice than normal where Maintenance is required in an emergency; and
- 6.2.4 may, in the event of a security breach affecting the Compute Protect server security Service, require you to change any or all of your passwords.

6.3 The End of the Service

On termination of the Compute Protect server security Service by either of us, BT:

- 6.3.1 will provide configuration information relating to the Compute Protect server security Service provided at the Site(s) in a format that BT reasonably specifies;
- 6.3.2 may delete any Content; and
- 6.3.3 will produce a final invoice for you within a month of the date of termination.

7 YOUR OBLIGATIONS

7.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Compute Protect server security Service, you will:

- 7.1.1 provide BT with the names and contact details of the Customer Contact, but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;
- 7.1.2 provide BT with any information reasonably required without undue delay;
- 7.1.3 complete any preparation activities that BT may request to enable you to receive the Compute Protect server security Service promptly and in accordance with any reasonable timescales; and
- 7.1.4 ensure that you have registered for access to the Portal and you hold a valid username and password for the Portal.

7.2 During Operation

On and from the Service Start Date, you will:

- 7.2.1 ensure that Users report Incidents to the Customer Contact and not to the Service Desk;
- 7.2.2 comply with any instructions BT gives you to allow you to access the Compute Protect server security Service;
- 7.2.3 ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and is available for all subsequent Incident management communications;
- 7.2.4 monitor and maintain any Customer Equipment connected to the Compute Protect server security Service or used in connection with a Compute Protect server security Service;
- 7.2.5 ensure that any Customer Equipment that is connected to the Compute Protect server security Service or that you use, directly or indirectly, in relation to the Compute Protect server security Service is:
 - (a) connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;

- (b) technically compatible with the Compute Protect server security Service and will not harm or damage BT Equipment, the BT Network, the Portal or any of BT's suppliers' or subcontractors' network or equipment; and
 - (c) 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;
- 7.2.6 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment does not meet any relevant instructions, standards or Applicable Law;
- 7.2.7 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Compute Protect server security Service;
- 7.2.8 maintain a written list of current Users and provide a copy of such list to BT within five Business Days following BT's written request at any time;
- 7.2.9 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Compute Protect server security Service and:
- (a) immediately terminate access for any person who is no longer a User;
 - (b) inform BT immediately 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;
 - (c) take all reasonable steps to prevent unauthorised access to the Compute Protect server security Service;
 - (d) satisfy BT's security checks if a password is lost or forgotten; and
 - (e) change any or all passwords or other systems administration information used in connection with the Compute Protect server security Service if BT requests you to do so in order to ensure the security or integrity of the Compute Protect server security Service.
- 7.2.10 regularly back up your data and computer systems on a separate media;
- 7.2.11 ensure that the maximum number of Users will not exceed the permitted number of User identities as set out in any applicable Order; and
- 7.2.12 not allow any User specific subscription to be used by more than one individual User unless it has been reassigned in its entirety to another individual User, in which case you will ensure the prior User will no longer have any right to access or use the Compute Protect server security Service.

8 NOTIFICATION OF INCIDENTS

Where you become aware of an Incident:

- 8.1 the Customer Contact will report it to the Service Desk;
- 8.2 BT will give you a Ticket;
- 8.3 BT will inform you when it believes the Incident is cleared and will close the Ticket when:
- 8.3.1 you confirm that the Incident is cleared within 24 hours after having been informed; or
 - 8.3.2 BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident, and you have not responded within 24 hours following BT's attempt to contact you.
- 8.4 If you confirm that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.

Part C – Service Levels

9 SERVICE LEVELS

There are no Service Levels for this Compute Protect server security Service.

Part D – Defined Terms

10 DEFINED TERMS

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

“Additional Terms” means any shrink-wrap, click-wrap, or other terms and conditions or agreements which you may need to accept when you install any third party software necessary for the functioning of the Compute Protect server security Service or any of the Software Modules.

“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.

“BT Price List” means the document containing a list of BT’s charges and terms that may be accessed at: www.bt.com/pricing (or any other online address that BT may advise you).

“Business Hours” means between the hours of 0800 and 1700 in a Business Day.

“Compute Management System” or **“CMS”** means the online portal and the automation / orchestration system that manages and drives the Compute Protect server security Service.

“Compute Protect server security Service” has the meaning given in Paragraph 1.

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

“Customer Contact” means any individuals authorised to act on your behalf for Compute Protect server security Service management matters.

“Customer Equipment” means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a Compute Protect server security Service.

“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.

“Enabling Service” has the meaning given in Paragraph 4.1.

“General Terms” means the general terms that this Schedule is attached to, or where not attached to this Schedule, can be found at www.bt.com/terms, and form part of the Contract.

“Incident” means an unplanned interruption to, or a reduction in the quality of, the Compute Protect server security Service or particular element of the Compute Protect server security Service.

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

“Internet Protocol” or **“IP”** means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.

“IP Address” means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.

“Monthly Allowance” means an upfront payment for the use of the Compute Protect server security Service on a specified number of Virtual Machines and for a certain number of hours in any given calendar month.

“Notice to Amend” has the meaning given in Paragraph 5.1.3.

“Packet” means the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

“Planned Maintenance” means any Maintenance BT has planned to do in advance.

“Portal” means the Compute Management System and the graphical user interfaces of the other BT services made available via the Compute Management System.

“Professional Services” means those services provided by BT which are labour related services.

“Security Modules” has the meaning given in Paragraph 2.1.

“Service Desk” means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Compute Protect server security Service.

“Service Management Boundary” has the meaning given in Paragraph 3.1.

“Site” means a location at which the Compute Protect server security Service is provided.

“Standard Service Components” has the meaning given in Paragraph 2.

“Stateful Firewall” means a firewall that keeps track of the state of network connections travelling across it. It allows you 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.

“Ticket” means the unique reference number provided by BT for an Incident and that may also be known as a **“fault reference number”**.

“Usage Charges” means the Charges for the Compute Protect server security Service or applicable part of the Compute Protect server security Service that are calculated by multiplying the volume of units that you used or incurred in a period (e.g. number of agents using the Compute Protect server security Service, or the number of minutes the Compute Protect server security Service was used for) with the relevant fee as set out in any applicable Order.

“Utility Rate Card” means information available via the Portal that shows the Charges for the Elements of the service on an hourly basis.

“Virtual Machine” or **“VM”** means a self-contained operating system that functions as a separate server.

“Virus Pattern Files” means a computer file used to help capture viruses.