



Managed Embedded Security Controls Service Annex to the BT Managed Security Service Schedule

Contents

Application of this Annex	2
A note on 'you'	2
Words defined in the General Terms	2
Part A – The Managed Embedded Security Controls Service	2
1 Service Summary	2
2 Standard Service Components	2
3 Service Options	3
4 Service Management Boundary	5
5 Associated Services and Third Parties	5
6 Specific Terms	5
Part B – Service Delivery and Management	7
7 BT's Obligations	7
8 Your Obligations	7
Part C – Service Levels	8
9 Service Care Levels	8
Part D – Defined Terms	9
10 Defined Terms	9



Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the Managed Embedded Security Controls Service. The terms of this Annex apply in addition to the terms set out in:

- (a) the Schedule; and
- (b) the General Terms.

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 Annex have the meanings given to them in the General Terms or the Schedule.

Part A – The Managed Embedded Security Controls Service

1 Service Summary

BT will provide you with a right to access Embedded Security Controls enabling you to protect your Users from threats from the Internet, comprising:

- 1.2 the Standard Service Components; and
- 1.3 any of the Service Options as set out in Paragraph 3 that are selected by you as set out in any applicable Order, up to the point of the Service Management Boundary as set out in Paragraph 4 ("**Managed Embedded Security Controls 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 Aggregated Bandwidth Consumption

2.1.1 BT will provide you with the availability of the following range of aggregated bandwidth consumptions to access the Internet required by you:

- (a) <100Mb;
- (b) 100Mb – 500Mb;
- (c) 500Mb – 1Gb;
- (d) 1Gb – 5Gb; or
- (e) 5Gb – 10Gb;

2.1.2 BT may monitor the aggregated Internet traffic bandwidth consumption used by you in accordance with the consumption purchased. BT may require you to purchase more aggregated bandwidth at an additional Charge where you go over your aggregated bandwidth consumption purchased. BT may not be able to provide you with the full Managed Embedded Security Controls Service if you do not purchase more aggregated bandwidth as required by BT.

2.2 Security Event Reporting:

- 2.2.1 BT will provide reporting facilities on-line which allows analysis of security-related events.
- 2.2.2 BT will not pro-actively view your reports and events for security incidents as part of this Standard Service Component.
- 2.2.3 If this Standard Service Component is delivered via a shared reporting platform, BT will configure the platform such that you are only provided with access to your reports. This may mean that some of the platform's functionality is restricted to preserve the confidentiality of all customers using that platform.
- 2.2.4 The period over which data can be analysed is dependent on the capacity of the Security Appliances or the space allocated on the reporting platform.
- 2.2.5 If you select the SSL/TLS Inspection Service Option set out in Paragraph 3.7, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

2.3 High Availability (dual appliance) solutions:

BT will configure the Managed Embedded Security Controls Service to provide resilience against multiple failures, utilising both hardware resilience with the Embedded Security Controls network nodes and failover between

Embedded Security Controls network nodes to ensure high availability of the Managed Embedded Security Controls Service.

2.4 Initial Setup

BT will as part of the Initial Setup:

- 2.4.1 commission the Embedded Security Controls and establish a remote link from your networked Customer Equipment to the Embedded Security Controls; and
- 2.4.2 monitor and manage the Embedded Security Controls in accordance with this Annex and the Schedule.

3 Service Options

BT will provide you with any of the following options ("**Service Options**") as set out in any applicable Order and in accordance with the details as set out in that Order.

3.1 URL Filtering and Application Control

3.1.1 BT will:

- (a) block access to the Internet sites that you ask BT to, in accordance with your CSP;
- (b) send an appropriate message to a User attempting to access a blocked or restricted Internet site to advise either:
 - (i) that the User request has been blocked; or
 - (ii) that the User will first confirm acceptance of your acceptable use policy (or similar warning) and upon acceptance by the User, the page will be delivered; and
- (c) implement any alterations, via the standard configuration management process, in the event of any change in your CSP.

3.2 Anti-Virus

3.2.1 BT will:

- (a) check web browser (http) traffic for known malware;
- (b) inspect requests from Users for an executable file from a site on the Internet, against the current antivirus definition file set out in the applicable intrusion signature files. If no virus is detected, the file will be passed to the User. If a virus is detected the file will be blocked and deleted; and
- (c) keep antivirus definition files up to date by regular downloads direct from the firewall supplier.

3.3 Anti-Bot

3.3.1 BT will check and block outbound traffic for communication with known command and control servers used by owners of malicious software.

3.4 VPNs

3.4.1 BT will set up and configure the following types of VPN in accordance with BT's prevailing technical standards:

- (a) remote access IPSec/SSL VPNs, for remote Users to gain secure access to your internal network. BT will implement your rules to authenticate against your authentication server. You are responsible for providing and installing your own end-user VPN software; and
- (b) Site to Site IP Sec VPNs between two Security Appliances managed by BT.

3.4.2 Where a digital certificate is required for remote VPN set up, either BT will provide, or you will provide to BT, as set out in the Order, an up-to-date digital certificate that will be installed on the Security Appliance.

3.4.3 Where you provide the digital certificate, BT will install it within seven days of receipt from you.

3.4.4 If you have selected Premium Graded Service Tier, BT will notify you of the date of expiry of the digital certificate three months prior to the date of expiry. You will advise BT, in writing, within one month of the date of BT's notification whether or not you want to renew your digital certificate.

3.4.5 If you want to renew your digital certificate and it is your responsibility as set out in the Order to provide BT with the digital certificate, you will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate.

3.4.6 BT will not be liable for issues caused by expired digital certificates if:

- (a) you do not confirm to BT that you want to renew your digital certificate in accordance with Paragraph 3.4.4; or
- (b) you do not provide BT with an up-to-date digital certificate in accordance with Paragraph 3.4.5.

3.5 Intrusion Detection and Prevention Service ("IPS")

- 3.5.1 BT will:
 - (a) monitor traffic passing through your Security Appliance for attacks, in accordance with the applicable intrusion signature files; and
 - (b) implement IPS with a default configuration setting, as defined by BT. BT will also maintain a subscription to the necessary signature updates, and arrange for these to be applied following issue by the supplier.
- 3.5.2 BT will not be responsible for evaluating these signatures beforehand.
- 3.5.3 BT will advise you how the IPS that you have selected operates with regard to alerting or IPS specific reporting.
- 3.5.4 If BT agrees a request from you to alter the parameters for applying new signatures in "**block**" mode to give a greater or lower sensitivity to attacks, you accept responsibility for the increased risk of false positives (blocks to legitimate traffic) or the increased risk of attacks being missed.
- 3.5.5 If you select the SSL/TLS Inspection Service Option set out in Paragraph 3.7, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.

3.6 Threat Emulation Service

- 3.6.1 The Threat Emulation Service will only be available if you have selected the Premium Graded Service Tier under the Schedule.
- 3.6.2 BT will encrypt suspected malicious files and send them to the vendor's cloud-based infrastructure where they will be decrypted and analysed for malware by reviewing its behaviour in a virtual environment (sandbox).
- 3.6.3 You may be able to choose whether to hold the file whilst it is being analysed (to provide increased security) or to release it and analyse it in the background (for improved User response). Background processing may lead to malicious files being permitted until signature updates are subsequently generated and applied to your Security Appliances.
- 3.6.4 If a file has been deemed malicious, its characteristics will be added to the vendor's anti-virus signature list.
- 3.6.5 BT will determine the country in which this inspection and analysis occurs.
- 3.6.6 If the SSL/TLS Inspection Service Option set out in Paragraph 3.7 is selected, BT will be able to scan SSL Encrypted Traffic in the same way that non-encrypted traffic can be scanned, provided your CSP permits such scanning.
- 3.6.7 Submission and processing of your data via the Threat Emulation Service will be at your sole discretion and at your own risk. Other than BT's obligations in Clause 14 of the General Terms, BT assumes no responsibility or liability for the receipt and processing of such data.

3.7 SSL/TLS Inspection

- 3.7.1 BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP).
- 3.7.2 BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.
- 3.7.3 The provisions set out in the Paragraphs 3.4.2 to 3.4.6, in relation to digital certificates apply to SSL/TLS Inspection.

3.8 Identity Awareness/User groups

- 3.8.1 The Identity Awareness/User groups Service Option will only be available if you have selected the Premium Graded Service Tier under the Schedule.
- 3.8.2 BT will configure the features of the Security Appliance that support the Identity Awareness/User groups to apply certain rules of the CSP according to the authenticated identity of the User rather than just their IP Address.
- 3.8.3 This may require client Software to be installed within your network or on end-user devices, or ensuring BT has remote, read-only, access to your active directory authentication server.
- 3.8.4 You will maintain the authentication database of Users, groups and any access credentials that you require.

3.9 Ad Hoc Professional Services

- 3.9.1 BT will provide ad hoc technical support or project management support, chargeable per day, as set out in the applicable Order.
 - 3.9.2 Professional Services are delivered remotely unless otherwise set out in the applicable Order.
- 3.10 Service Options may not be available in all countries.

4 Service Management Boundary

- 4.1 BT will provide and manage the Managed Embedded Security Controls Service as set out in Parts A, B and C of this Annex and as set out in the Order. The service management boundary is the point where traffic enters and leaves the infrastructure owned or controlled by BT ("**Service Management Boundary**").
- 4.2 BT will have no responsibility for the Managed Embedded Security Controls Service outside the Service Management Boundary including:
 - 4.2.1 issues on User machines (e.g. operating system, coding languages and security settings);
 - 4.2.2 end to end network connectivity (e.g. your network or networking equipment, Internet connectivity);
 - 4.2.3 identity source management;
 - 4.2.4 policy ownership; or
 - 4.2.5 security information and event management analysis.
- 4.3 BT does not guarantee that the Managed Embedded Security Controls Service will detect or block all malicious threats.
- 4.4 BT does not make any representations, whether express or implied, about whether the Managed Embedded Security Controls Service will operate in combination with any Customer Equipment or other equipment and software, unless agreed with BT.

5 Associated Services and Third Parties

- 5.1 You will provide and maintain an Internet connection at the Site(s) at all times for use with the Managed Embedded Security Controls Service, including providing and maintaining any Customer Equipment necessary for such connection. You will pay all charges related to provision, maintenance and use of such Internet connections and report any incidents on the Internet connections directly to the supplier of the compatible Internet connections.
- 5.2 If BT provides you with additional services this Annex will not apply to those services and those services will be governed by their separate terms and conditions.
- 5.3 BT will not be liable for failure to or delay in supplying the Managed Embedded Security Controls Service if another supplier delays or refuses the supply of an electronic communications service to BT and no alternative service is available at reasonable cost.

6 Specific Terms

6.1 Service Amendment

In addition to what is set out in Clause 31 of the General Terms:

- 6.1.1 throughout the Minimum Period of Service, you may request an increase or decrease of the aggregated bandwidth consumption supplied, subject to capacity and the current bandwidth consumption by you;
 - 6.1.2 any bandwidth increase or decrease will be chargeable by BT and will operate for a minimum period of five Business Days before you may make any further requests; and
 - 6.1.3 where a bandwidth increase is beyond the available capacity of your current Managed Embedded Security Controls Service, BT will ensure your IPsec tunnels are re-routed via a different IP Address. BT may require you to change your IP Address.
- 6.2 **Invoicing**
- 6.2.1 BT may invoice you for any of the following Charges in addition to those set out in the Schedule or any applicable Order:
 - (a) an increase or decrease of the aggregated bandwidth consumption in accordance with Paragraphs 2.1.2 and 6.1 of this Annex.

6.3 Amendments to the BT Managed Security Service Schedule

- 6.3.1 Paragraph 6.2 of the Schedule will not apply.
- 6.3.2 Regardless of what it may say in Paragraph 9.1 of the Schedule:
 - (a) at the end of the Minimum Period of Service, unless one of us has given Notice to the other of an intention to terminate the Managed Embedded Security Controls Service in accordance with the

- Contract, BT will continue to provide the Managed Embedded Security Controls Service and each of us will continue to perform our obligations in accordance with the Contract;
- (b) if the Managed Embedded Security Controls Service is the only Associated Service purchased under the Contract for the BT Managed Security Service, Paragraph 9.1 of the Schedule will not apply to the BT Managed Security Service and Paragraph 6.3.2 will apply; and
 - (c) if the Managed Embedded Security Controls Service is purchased along with other Associated Services under the Contract for the BT Managed Security Service, Paragraph 9.1 of the Schedule will apply to the BT Managed Security Service and the other Associated Services and Paragraph 6.3.2(a) will apply only to the Managed Embedded Security Controls Service.
- 6.3.3 The wording in Paragraph 9.5.2 of the Schedule is deleted and replaced with the following:
- 9.5.2 In addition to the Charges set out at Paragraph 9.5.1 above, if you terminate the Managed Embedded Security Controls Service during the Minimum Period of Service you will pay BT:
- (a) for any parts of the Managed Embedded Security Controls Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service; and
 - (b) any fees, charges, or costs paid by BT to a supplier that cannot be recovered from the supplier.



Part B – Service Delivery and Management

7 BT's Obligations

7.1 Commissioning of the Service

Before the Service Start Date, BT will provide IP Addresses for you to connect your customer networking equipment to the IPSec tunnel and ensure BT can receive Internet traffic from you.

7.2 The End of the Service

On termination of the Managed Embedded Security Controls Service by either of us, BT will terminate your access to the Embedded Security Controls and cease to provide all other elements of the Managed Embedded Security Controls Service.

8 Your Obligations

8.1 Service Delivery

Before the Service Start Date and, where applicable, throughout the provision of the Managed Embedded Security Controls Service, you will:

- 8.1.1 ensure that the LAN protocols and applications you use are compatible with the Managed Embedded Security Controls Service;
- 8.1.2 establish and maintain your own internal support processes and helpdesk for Users and be responsible for communication with Users;
- 8.1.3 ensure that your firewall configurations and network settings allow the traffic types necessary for BT to provide the Managed Embedded Security Controls Service, including:
 - (a) ensuring that external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) are set up to be directed through the Managed Embedded Security Controls Service by making and maintaining the configuration settings required to direct external traffic via the Managed Embedded Security Controls Service, with BT's assistance and support as reasonably required and you acknowledge that this external traffic is dependent on your technical infrastructure; and
 - (b) ensuring that internal HTTP, HTTPS and FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Managed Embedded Security Controls Service;
- 8.1.4 ensure that you order the appropriate Managed Embedded Security Controls Service features for your requirements;
- 8.1.5 provide BT with the WAN/LAN IP Address to enable BT to connect you to the Managed Embedded Security Controls Service;
- 8.1.6 manage, and provide BT with accurate details of your internal IP Address design;
- 8.1.7 modify your network routing to ensure appropriate traffic is directed to the Embedded Security Controls;
- 8.1.8 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request;
- 8.1.9 configure your devices to enable them to connect to the Managed Embedded Security Controls Service; and
- 8.1.10 ensure that your Internet traffic can be routed through the Managed Embedded Security Controls Service.

8.2 During Operation

On and from the Service Start Date, you will:

- 8.2.1 provide BT with Notice 14 days in advance of any changes to your network that may impact the working of the Managed Embedded Security Controls Service and provide BT with all necessary details. If this information is not provided within this timeframe, BT will have no liability for a failure or delay in providing any necessary changes to the Managed Embedded Security Controls Service configuration;
- 8.2.2 ensure that your Internet traffic can be routed through the Managed Embedded Security Controls Service; and
- 8.2.3 change your IP Address when requested by BT in accordance with Paragraph 6.1.3.

8.3 The End of the Service

On termination of the Managed Embedded Security Controls Service by either of us, you will disconnect the IPSec tunnel on your customer networking equipment from BT's Embedded Security Controls, otherwise your Internet bound traffic may not work.



Part C – Service Levels

9 Service Care Levels

There are no specific Service Levels for this Managed Embedded Security Controls Service.

Part D – Defined Terms

10 Defined Terms

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

"Cardholder Data" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

"Customer Equipment" means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a Managed Embedded Security Controls Service.

"De-installation Charges" means the charges payable by you on de-installation of the Managed Embedded Security Controls Service that are equal to the then current rates for Installation Charges on the date of de-installation.

"Domain Name System" or **"DNS"** is a hierarchical and decentralised naming system for computers, services, or other resources connected to the Internet or a private network.

"Embedded Security Controls" means a software based network security system that uses rules to control incoming and outgoing network traffic.

"Enabling Service" has the meaning given in Paragraph 5.1.

"EU" means European Union.

"File Transfer Protocol" or **"FTP"** means standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

"File Transfer Protocol Secure" or **"FTPS"** means the name used to encompass a number of ways in which FTP software can perform secure file transfers. Each involves the use of a security layer below the standard FTP protocol to encrypt data.

"General Terms" means the general terms to which this Schedule is attached or can be found at www.globalservices.bt.com/en/terms-and-conditions, and that form part of the Contract.

"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.

"Identity Awareness/User groups" means the Service Option as set out in Paragraph 3.8.

"Incident" means an unplanned interruption to, or a reduction in the quality of, the Managed Embedded Security Controls Service or particular element of the Managed Embedded Security Controls Service.

"Internet Message Access Protocol Secure" or **"IMAPS"** is a mail protocol used to receive emails from a remote server to a local email client.

"IPS" means intrusion detection and prevention service.

"IPSec" means Internet Protocol security; it is a standards-based framework that provides layer 3 services for confidentiality, privacy, data integrity, authentication and replay prevention.

"MAC address" means media access control address, a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

"Managed Embedded Security Controls Service" has the meaning given in Paragraph 1.

"Post Office Protocol 3 Secure" or **"POP3S"** is a standard mail protocol used to receive emails from a remote server to a local email client.

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

"Schedule" means the BT Managed Security Service Schedule to the General Terms.

"Service Management Boundary" has the meaning given in Paragraph 4.1.

"Service Options" has the meaning given in Paragraph 3.

"Simple Mail Transfer Protocol" or **"SMTP"** is a communication protocol for electronic mail transmission.

"Simple Mail Transfer Protocol Secure" or **"SMTPS"** is a method for securing the SMTP using transport layer security.

"Site" means a location at which the Managed Embedded Security Controls Service is provided.

"SSL" means secure sockets layer.

"SSL Encrypted Traffic" means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

- (a) HTTPS;
- (b) SMTPS;
- (c) POP3S;
- (d) IMAPS; and

(e) FTPS.

“**SSL/TLS Inspection**” means the Service Option as set out in Paragraph 3.7.

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

“**Threat Emulation Service**” means the Service Option as set out in Paragraph 3.6.

“**VPN**” means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over network infrastructure that is shared with other customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.

“**WAN**” means wide area network.