BT Managed CrowdStrike Falcon XDR® Service Annex to the Managed Service Schedule

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the BT Managed CrowdStrike Falcon XDR® 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 and the Schedule.

Part A – The BT Managed CrowdStrike Falcon XDR® Service

1. Service Summary

1.1 BT will provide you with a cloud- based endpoint detection and response service, utilising the CrowdStrike Falcon endpoint security technology, comprising of:

1.1.1. A set of Standard Service Components; and

1.1.2. Any applicable Service Options, as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 ("**BT Managed CrowdStrike Falcon XDR® Service**" or ("**BT CrowdStrike XDR® Service**").

2. Standard Service Components

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

2.1 **CrowdStrike Licence Pack**

The CrowdStrike Licence Pack includes the CrowdStrike Software licenses set out in your Managed Service Order, which you will be able to roll out to all of the endpoints covered within your service. If you purchase further licenses throughout the duration of your Contract, these licenses will terminate at the same time as your existing Contract.

2.2 **CrowdStrike Falcon Portal**

The CrowdStrike Falcon Portal is a portal which BT will manage on your behalf. The BT Security Operations Centre will monitor potential Security Incidents and provide recommendations to you on threat Mitigating Actions that you may take to protect your endpoint Devices.

2.3 **First Line Support – Service Desk**

The first line support (Service Desk) will be available 24x7x365 to raise any issues with your Service. The Service Desk will work through structured questions to assess the severity of the issue and if it can't be resolved, the Service Desk will raise an Incident Ticket to the Security Operations Centre team for support.

2.4 **Second Line Support – Security Analysts within the SOC**

2.4.1 The Second Line Support comprises of two different layers of Security Operations support teams, that will:

(a) monitor security alerts generated by CrowdStrike Falcon Portal;
(b) determine critical system and data integrity;
(c) if you have selected an MS1 Package, BT will make recommendations of suggested Mitigating Action that you can take to protect against security threats;
(d) if you have selected an MS2 Package or MS3 Package, BT will automatically take Mitigating Action against security threats when pre- agreed; should any Mitigating Actions need to be taken which have not been pre-agreed, the BT Security Operations Centre will reach out to you for your approval; and

(e) escalate to the third line support, critical issues to CrowdStrike if necessary.

2.5 **Third Line Support – Supplier Support Team**

Third line support (provided by the Supplier) will deal with escalations from second line support (provided by BT) as set out in Paragraph 2.4, and use the investigations carried out by BT to support an Incident or Security Incident effectively.

2.6 **Falcon Agent**

The Falcon Agent is a lightweight, cloud-native endpoint software sensor that forms the foundation of the CrowdStrike Falcon Platform. It is designed, in conjunction with the CrowdStrike Falcon Platform, to deliver comprehensive security capabilities through a single, unified agent.

3. Managed Service Packages

3.1 You will choose one of the Managed Service Packages, some of the features of which are set out in the tables below, as set out in any applicable Order. The Managed Service Package you have chosen for the Managed CrowdStrike Falcon XDR® Service must align with the Managed Service Package you have chosen for your overall Managed Service, as set out in the Schedule.

CrowdStrike Falcon Module / Functionality	MS1	MS2	MS3
Prevent / Next generation anti-virus	Included		
Insight XDR / Extended detection & response	Included		
Intelligence / Falcon threat intelligence feed and Sandbox	Included		
Threat Graph Std / Security data store & analysis (7d)	Included		
Eagle-i	N/A	Included	
BT CySOC Incident Mitigation	N/A	Included	
Identity Threat Protection / Identity security	N/A	Optional	Optional
Cloud Security / CSPM and CWP functionality	N/A		Optional
Falcon Additional Data Retention functionality	N/A		Optional
Falcon Data Ingestion functionality	N/A		Optional
Falcon Search Retention functionality	N/A		Optional
Integration of Third-Party Security Solutions	N/A		Optional
Falcon for Mobile / Protection for iOS and Android devices	Optional		
Firewall Management / Software endpoint firewall	Optional		
Device Control / USB device control	Optional		
Discover / IT hygiene	Optional		
Spotlight / Vulnerability insight	Optional		
Overwatch / Integrated analyst threat hunting	Optional		
Sandbox / Extended Sandbox queries (250 per month)	Optional		
Threat Graph Extended Data Storage / 30,60,90,180 or 365 days	Optional		

3.2 **Incident Mitigation**

3.2.1 Incident Mitigation is part of the MS2 Package and MS3 Package. Following the provision of an Incident alert the BT Security Operations Centre shall automatically implement any Mitigating Action in respect of the specific endpoint Device which has been affected by the Security Incident, subject to Paragraphs 3.2.2 and 3.2.3.

3.2.2 If you have selected the MS3 Package, then Incident Mitigation also allows the BT Security Operations Centre to automatically quarantine an endpoint Device which has been compromised by the Security Incident in order to stop the Security Incident from spreading further. It will be your responsibility to perform remediating action on the Device and then it will also be your responsibility to confirm to BT when you have completed this action so BT can remove the Device from quarantine. BT will not incur any liability arising out of improper or incomplete remediating action performed on your Device by you.

3.2.3 You will agree with BT which specific endpoint Devices are in-scope of the Managed CrowdStrike Falcon XDR® Service, and for which BT can automatically take Mitigating Action, in writing in a policy document signed by you.BT shall not be responsible for any impact on endpoint Devices, Customer Equipment, or your wider Network, of Mitigating Action which BT takes on a specific endpoint Device(s), where you have

not identified to BT that it should not in fact take automatic Mitigating Action in respect of that specific endpoint Device(s).

3.3 Dependent on the Managed Service Package which you have chosen, you will be provided with support from BT as set out in the table below:

	MS1 Package	MS2 Package	MS3 Package
BT Support			
Technical Implementation	✓	✓	✓
Project Management	✓	✓	✓
Alert configuration	✓	✓	✓
Change management	✓	✓	✓
Service desk	✓	✓	✓
TAM reporting	6 monthly	Quarterly	Monthly
Security Incident log retention	7 days	7 days or as agreed by the Parties	7 days or as agreed by the Parties

4. Service Management Boundary

4.1 BT will provide and manage the Managed CrowdStrike Falcon XDR® Service in accordance with Parts A, B and C of this Annex and as set out in any applicable Order up to the CrowdStrike Falcon Portal in the cloud ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Managed CrowdStrike Falcon XDR® Service outside the Service Management Boundary.

4.3 BT does not make any representations, whether express or implied, about whether the Managed CrowdStrike Falcon XDR® Service will operate in combination with any Customer Equipment or other equipment and Software.

5. Associated Services

5.1 You will have the following services in place that will connect to the Managed CrowdStrike Falcon XDR® Service which is necessary for the Managed CrowdStrike Falcon XDR® Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 an IP connection allowing Managed CrowdStrike Falcon XDR® Service to connect to the cloud based CrowdStrike Falcon Portal; and

5.1.2 an Internet connection with sufficient bandwidth,

(each an "**Enabling Service**").

5.2 The Managed CrowdStrike Falcon XDR® Service will only operate on certain operating systems which will be advised by BT and can be found at https://www.crowdstrike.com/endpoint-security-products/crowdstrike-falcon-faq/.

5.3 If BT provides you with any services other than the Managed CrowdStrike Falcon XDR® Service (including, but not limited to any Enabling Service) this Annex will not apply to those services and those services will be governed by their separate terms.

6. Equipment

BT does not make any representations, whether express or implied, about whether the Managed CrowdStrike Falcon XDR® Service will operate in combination with any Customer Equipment or other equipment and Software.

7. Specific Terms

7.1 **Customer Committed Date**

7.1.1 If you request a change to the Managed CrowdStrike Falcon XDR® Service or any part of the Managed CrowdStrike Falcon XDR® Service, then BT may revise the Customer Committed Date to accommodate that change.

7.1.2 BT may expedite delivery of the Managed CrowdStrike Falcon XDR® Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

7.2 **EULA**

7.2.1 BT will only provide the Managed CrowdStrike Falcon XDR® Service if you have accepted the end user licence agreement with the Supplier in the form set out at CrowdStrike Terms And Conditions | CrowdStrike, as may be amended or supplemented from time to time by the Supplier ("**EULA**"). By entering into this Contract, you accept the terms of the EULA.

7.2.2 You will observe and comply with the EULA for all and any use of the applicable Software.

7.2.3 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the Managed CrowdStrike Falcon XDR® Service upon reasonable Notice, and:

(a) you will continue to pay the Charges for the Managed CrowdStrike Falcon XDR® Service until the end of the Minimum Period of Service or Renewal Period; and

(b) BT may charge a re-installation fee to re-start the Managed CrowdStrike Falcon XDR® Service.

7.2.4 You will enter into the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between you and the Supplier and you will deal with the Supplier with respect to any loss or damage suffered by either of you as such loss or damage will not be recoverable from BT.

7.2.5 Where the EULA is presented in a 'click to accept' function and you require BT to configure or install Software on your behalf, BT will do so as your agent and bind you to the EULA.

7.2.6 You acknowledge and agree that any Third-Party Security Solutions that you will integrate into your Managed CrowdStrike Falcon XDR® service are solely your responsibility. Any integrations must follow any relevant guidelines made available by the Supplier

7.2.7 You are responsible for conducting due diligence on any Third-Party Security Solution vendors to ensure they meet your security standards.

7.2.8 BT shall not be liable for any issues arising from the integration of third-party data sources, including but not limited to data breaches, service interruptions, or performance degradation.

7.3 **Reviews**

7.3.1 MS1 Package

(a) The Threat Analytics Manager will carry out a review six monthly as follows:

(i) a Managed CrowdStrike Falcon XDR® Service review focussing on the performance of the Managed CrowdStrike Falcon XDR® Service; and

(ii) an 'end of life' review on an ongoing basis. The Threat Analytics Manager will provide you with a report summarising the applications and Software that are managed by BT on your behalf as part of the Managed CrowdStrike Falcon XDR® Service that will become end of life within the following six months. The report will include applications and Software advised to you previously that are past end of life and that require immediate action by you.

(b) If requested by you and if agreed to by BT, both of us may hold a conference call to discuss the report.

(c) If BT has agreed to participate in a conference call you will ensure that any report the Threat Analytics Manager provides you with will be reviewed by your suitably qualified personnel who are participating in the conference call prior to the conference call taking place.

(d) You will take appropriate action to address issues as recommended by the Threat Analytics Manager:

(i) in respect of the Managed CrowdStrike Falcon XDR® Service including implementing security improvements as agreed with the Threat Analytics Manager or as advised by the Threat Analytics Manager as your responsibility; and

(ii) in respect of the end of life review or as set out in the end of life review report.

7.3.2 MS2 Package

(a) The Threat Analytics Manager will carry out a review quarterly as follows:

(i) a Managed CrowdStrike Falcon XDR® Service review focussing on the performance of the Managed CrowdStrike Falcon XDR® Service;

(ii) a review of your CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of your CSP(s); and

(iii) an end of life review as set out in Paragraph (ii).

(b) In addition to taking the action set out in Paragraph 7.3.1 (d), you will be responsible for initiating the appropriate change requests in accordance with the CSP Change Management Process to address issues in respect of fine tuning or amending your CSP(s) as recommended by the Threat Analytics Manager.

7.3.3 MS3 Package

(a) The Threat Analytics Manager will carry out a review at intervals agreed by both of us but not less than monthly as follows:

(i) a Managed CrowdStrike Falcon XDR® Service review every month focussing on the performance of the Managed CrowdStrike Falcon XDR® Service;

(ii) a review of your CSP(s) focussing on the effectiveness of the rules applied to the CSP(s) and the need to fine tune or amend the rules of your CSP(s); and

(iii) an end of life review as set out in Paragraph (ii).

(b) The Threat Analytics Manager will provide you with a report on the review via the Security Portal or direct to you by e-mail, if agreed by both of us.

(c) If requested by you and if agreed to by BT, both of us may hold a conference call to discuss the report or BT may attend a meeting at your Site depending on your location to discuss the report with you.

(d) If BT has agreed to participate in a conference call or attend a meeting at your Site, you will ensure that any report the Threat Analytics Manager provides you with will be reviewed by your suitably qualified personnel who are participating in the conference call or attending the meeting prior to the conference call or meeting taking place.

7.4 **Upgrades/Downgrades to a Higher/Lower Managed Service Package**

7.4.1 There will be no upgrades/downgrades of the Managed Service Package available as your service tier must remain the same for the duration of your Contract.

7.5 **Amendments to the Managed Service Schedule**

7.5.1 Paragraphs, 2.5 (**Maintenance Care Levels**), 2.7 (**Vital Port Monitoring**), 2.8 (**In-Band and Out of Band Management**), 2.9 (**Configuration Management**) and 2.10 (**Software Upgrades**) of the Schedule will not apply.

7.5.2 Paragraphs 2.11.3 (**Network Reporting**), 2.11.4 (**IPSLA Reporting**) and 2.11.5 (**Application Reporting**) of the Schedule will not apply.

7.5.3 Paragraph 2.11.6 (**Vendor Network and Application Reporting**) of the Schedule will not apply if you have selected the MS1 Package but if you have selected either the MS2 or MS3 Package, your reports will be generated by the TAM.

7.5.4 Paragraphs 2.12 (**Capacity Management**) and 2.13 (**Availability Management**) of the Schedule will not apply.

7.5.5 Paragraph 2.14 (**Change Management – Simple Service Requests)** in the Schedule is deleted and replaced with the following:

2.14.1 BT will provide secure access to the Security Portal to all pre-agreed and authorised Customer Contacts to enable you to submit your change requests.

2.14.2 BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change and the status will be available also on the Security Portal for a period of six months.

2.14.3 BT will apply the following "reasonable use" restrictions ("Reasonable Use Policy") for changes to the CSP(s):

(i) you will not raise SSRs requests more frequently than:

(a) 10 per quarter in respect of MS 1; and

(b) 15 per quarter in respect of MS 2;

for MS 3 there be no limit of raised SSRs per quarter.

2.14.4You are deemed to have approved all changes to the CSP(s) that you submit to BT.

2.14.5 You are responsible for the impact of BT implementing the changes and BT is not liable for any consequences arising from the impact of the implementation of the changes.

7.5.6 Paragraph 2.16.5 (**WLAN Survey**), 2.16.6 (**Network Assessment Physical Detail Collection Package and Network Assessment Physical Detail Collection Day Rate**), 2.16.7 (**Infrastructure Cabling**) and 2.16.8 (**PDS Installation Services**) of the Schedule will not apply.

7.5.7 The wording of Paragraph 4.1 (**Changes to the Contract**) of the Schedule is deleted and replaced with the following:

4.1.1 BT may propose changes to this Schedule, the General Terms or the Charges (or any of them) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

4.1.2 Within 10 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 beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

4.1.3 If we have not reached agreement in accordance with Paragraph 4.1.2(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Schedule will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 4.1.2(c) or BT may give Notice of termination, in which case BT will cease delivering the Managed CrowdStrike Falcon XDR® Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.5.8 Regardless of what it may say in Paragraph 4.2 (**Minimum Period of Service and Renewal Periods**) of the Schedule:

4.2.1 You may request an extension to the Managed CrowdStrike Falcon XDR® Service for a Renewal Period by Notice in writing to BT at least 90 days before the end of the Minimum Period of Service or Renewal Period ("**Notice of Renewal**").

4.2.2 If you issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will extend the Managed CrowdStrike Falcon XDR® Service for the Renewal Period and both of us will continue to perform each of our obligations in accordance with the Contract.

4.2.3 If you do not issue a Notice of Renewal in accordance with Paragraph 4.2.1, BT will cease delivering the Managed CrowdStrike Falcon XDR® Service at the time of 23:59 on the last day of the Minimum Period of Service or Renewal Period.

4.2.4 If the Managed CrowdStrike Falcon XDR® Service is the only Associated Service purchased under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will not apply to the Managed Service and Paragraph 7.5.8 of this Annex will apply; and

4.2.5 If the Managed CrowdStrike Falcon XDR® Service is purchased along with other Associated Services under the Contract for the Managed Service, Paragraph 4.2 of the Schedule will apply to the Managed Service and the other Associated Services and Paragraph 7.5.8 of this Annex will apply only to the Managed CrowdStrike Falcon XDR® Service.

7.5.9 The wording in Paragraph 4.7.2 (**Termination Charges**) of the Schedule is deleted and replaced with the following:

4.7.2 In addition to the Charges set out at Paragraph 4.7.1 above, if you terminate the Managed CrowdStrike Falcon XDR® Service during the Minimum Period of Service or any Renewal Period you will pay BT:

(a) for any parts of the Managed CrowdStrike Falcon XDR® Service that were terminated during the Contract, Termination Charges, as compensation, equal to:

(i) 100 per cent of the Recurring Charges that are attributable to the CrowdStrike Licence Pack for the remaining Minimum Period of Service or any Renewal Period;

(ii) 100 per cent of the Recurring Charges that are attributable to the Managed Service, excluding those attributable to the CrowdStrike Licence Pack, for the first 12 months of the Minimum Period of Service;

(iii) 35 per cent of the Recurring Charges that are attributable to the Managed Service, excluding those attributable to the CrowdStrike Licence Pack, for the remaining Minimum Period of Service or Renewal Period; and

(iv) any waived Installation Charges;

7.5.10 Regardless of what it may say in Paragraphs 4.3.2 and 4.3.3 of the Schedule, if either of us terminates the Managed Service in accordance with Paragraph 4.3.1 of the Schedule, the Managed CrowdStrike Falcon XDR® Service will automatically terminate at the same time and you will pay Termination Charges in accordance with Paragraph 4.7 of the Schedule as amended by this Annex.

7.5.11 Paragraph 4.10 (**Security**) of the Schedule will not apply.

7.5.12 Paragraphs 5.1.3 (**BT obligations for PDS Installation**) and 5.3 (**BT's obligations During Operation**) of the Schedule will not apply.

7.5.13 Paragraphs 6.1.4 (**providing BT access to any of your Sites**), 6.1.6 (**specialist equipment at your Site**), 6.1.9 (**LAN protocols and applications compatible with the Managed Service and Associated Service**) and 6.2.13 (**your obligations on expiry or termination of the Managed Service**) of the Schedule will not apply.

7.5.14 Paragraphs 6.3 (**UCC Obligations**), 6.4 (**WAN Obligations**) and 6.5 (**LAN Obligations**) of the Schedule will not apply.

7.5.15 The wording in Paragraph 7 (**Notification of Incidents**) of the Schedule is deleted and replaced with the following:

7.1 Where you become aware of an Incident or a Security Incident:

7.1.1 The Customer Contact will report it to the Service Desk;

7.1.2 BT will give you a Ticket;

7.1.3 BT will inform you when it believes the Incident or Security Incident is cleared and will close the Ticket when:

(a) you confirm that the Incident or Security Incident is cleared within 24 hours after having been informed; or

(b) BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident or Security Incident, and you have not responded within 24 hours following BT's attempt to contact you.

7.1.4 If you confirm that the Incident or Security 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 or Security Incident.

7.1.5 Where BT becomes aware of an Incident or Security Incident, Paragraphs 7.1.2, 7.13 and 7.1.4 as amended by Paragraph 7.5.15 of this Annex will apply.

7.1.6 This Paragraph 7 will not apply to Security Incidents if you have selected the MS1 Package.

7.5.16 Part C (**Service Levels**) of the Schedule will be deleted and Part C of this Annex will apply instead.

7.6 **Amendments to the General Terms**

The definition of Software is deleted and replaced with:

"**Software**" means any software in object code format only, and related documentation (whether on tangible or intangible media) that BT or the Supplier provides to you as part of a Service. It includes any embedded software, but it excludes Open Source Software.

Part B – Service Delivery and Management

8. BT's Obligations

8.1 **During Operation**

On and from the Service Start Date, BT:

8.1.1 will respond and use reasonable endeavours to remedy an Incident or Security Incident without undue delay and in accordance with the Service Care Levels in Part C of this Annex if BT detects or if you report an Incident or Security Incident;

8.1.2 will maintain or arrange for the CrowdStrike Falcon Portal to be maintained to provide you with online access to performance reports;

8.1.3 may, in the event of a security breach affecting the Managed CrowdStrike Falcon XDR® Service, require you to change any or all of your passwords and

8.1.4 will generate and securely store the CrowdStrike Falcon credentials needed to establish the integration between Managed CrowdStrike Falcon XDR® Service and any Third-Party Security Solution.

8.2 **The End of the Service**

On termination of the Managed CrowdStrike Falcon XDR® Service by either of us, BT will terminate any rights of access to the CrowdStrike Falcon Portal and the Security Portal and stop providing all other elements of the Managed CrowdStrike Falcon XDR® Service.

9. Your Obligations

9.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Managed CrowdStrike Falcon XDR® Service, you will:

9.1.1 request that BT configures no more than 100 static or dynamic groups;

9.1.2 be responsible for downloading the CrowdStrike Licence Pack, and deploying licensed agent Software to the endpoint Devices selected;

9.1.3 use best endeavours to remediate any problems encountered during the process of deploying the licensed agent Software to the endpoint Devices selected;

9.1.4 provide consent for detection assessment and mitigation of the condition of the endpoint Device;

9.1.5 provide consent for sending logs in the form of metadata to the CrowdStrike Falcon Portal;

9.1.6 be responsible for establishing communication by opening ports and by-passing proxies between the deployed licensed agent Software and the Managed CrowdStrike Falcon XDR® Service;

9.1.7 identify which employees will have access to the Managed CrowdStrike Falcon XDR® Service, supply BT with their name and email address in order that their individual role based access can be created;

9.1.8 upon receiving the Managed CrowdStrike Falcon XDR® Service access credentials, ensure you successfully complete the account set-up, including password creation;

9.1.9 share with BT any relevant internal processes or policies that may affect delivery of the Managed CrowdStrike Falcon XDR® Service, and operations, and BT will advise where these are not compatible with the Managed CrowdStrike Falcon XDR® Service;

9.1.10 make available to BT sufficient resources to facilitate ordering, design, and implementation of the Managed CrowdStrike Falcon XDR® Service and/or the Third-Party Security Solutions;

9.1.11 nominate a representative(s) for SOC interaction when raising Incidents or Security Incidents;

9.1.12 where the Mitigation Service applies, identify to BT which of your endpoint Devices BT is authorised to automatically implement any Mitigating Action towards;

9.1.13 update the policies for any endpoint Devices which you have identified to BT as being within scope of the Mitigation Service, so that BT may access and automatically implement any Mitigating Action in respect of those endpoint Devices;

9.1.14 fulfil all these obligations that include but not limited to identifying to BT in advance of commencement of the Services (as well as keeping BT informed during the Services) of the specific endpoint Devices to which BT is authorised to automatically take Mitigating Action; and

9.1.15 generate and securely store the Third-Party Security Solution's credentials needed to establish the integration between Managed CrowdStrike Falcon XDR® Service and any the Third-Party Security Solution.

9.2 **During Operation**

On and from the Service Start Date, you will:

9.2.1 monitor and maintain any Customer Equipment connected to the Managed CrowdStrike Falcon XDR® Service or used in connection with the Managed CrowdStrike Falcon XDR® Service;

9.2.2 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law;

(b) contains or creates material that is in breach of the Acceptable Use Policy and you are contacted by BT about such material, and

redress the issues with the Customer Equipment prior to reconnection to the Managed CrowdStrike Falcon XDR® Service;

9.2.3 provide consent to BT permitting BT super administrator access; and

9.2.4 ensure that the data being sent from any Third-Party Security Solution to the Managed CrowdStrike Falcon XDR® Service complies with standards that may apply to your organisation.

Part C – Service Care Levels

10. Service Care Levels

10.1 All Incidents and Security Incidents will be assigned a Priority by BT. You may request, and BT will reasonably consider, changes to the Priority assigned to an Incident or Security Incident.

10.2 You will ensure that any Incident or Security Incident notification includes all relevant and available logs at the time of contacting BT.

10.3 BT may require additional data while investigating the Incident or Security Incident that could include:

10.3.1 WPP logs;

10.3.2 complete dumps (not mini-dumps);

10.3.3 packet captures - required to investigate firewall, application control, Device control issues;

10.3.4 machine image - when issue cannot be reproduced readily;

10.3.5 performance monitor logs;

10.3.6 process monitor logs;

10.3.7 windows performance analyser;

10.3.8 filemon logs; and

10.3.9 remote access to your endpoint Devices.

10.4 **Service Care Support**

10.4.1 Target Initial Response Time and Follow-Up

Priority Level	Target Initial Response Time	Follow-Up	Description and Examples
P1	• MS1 Package Support – whenever a progress update is available • MS2 Package Support and MS3 Package Support – confirmation of the Incident or Security Incident within 1 hour of the Incident or Security Incident being reported by telephone to the Service Desk	Every hour	• CrowdStrike Falcon Portal is not available to you. • Serious impact and Incident cannot be circumvented, typically where the Managed CrowdStrike Falcon XDR® Service is completely down / unavailable. • Large impact on a portion of the Managed CrowdStrike Falcon XDR® Service and cannot be circumvented, causes significant loss of the Managed CrowdStrike Falcon XDR® Service, but the impacted business function is not halted.
P2	• MS1 Package Support - whenever a progress update is available • MS2 Package Support and MS3 Package Support – confirmation of the Incident or Security Incident within 4 hours of the Incident or Security Incident being reported by telephone to the Service Desk	Every 8 hours	• CrowdStrike Falcon Portal is experiencing a degradation, but the CrowdStrike Falcon Portal is still available to you. • Small impact on the Managed CrowdStrike Falcon XDR® Service or where a single User or component is affected and it causes some impact to your business; for example: there is an intermittent or occasional disturbance which does not have a major impact on the

			Managed CrowdStrike Falcon XDR® Service. • Minor or intermittent impact to a non-operational element of the Managed CrowdStrike Falcon XDR® Service; for example: a temporary failure of reporting.
P3	• MS1 Package Support – whenever a progress update is available • MS2 Package Support and MS3 Package Support – confirmation of the Incident or Security Incident within 4 Business Hours of the Incident or Security Incident being reported.	Every 2 Business Days	• General questions. • Access requests to CrowdStrike Falcon Portal.

10.5 MS1 Package support provides support set out in the table at Paragraph 10.4.1 and will also include email communications, access to the CrowdStrike Falcon Portal and documented troubleshooting and technical assistance.

10.6 MS2 Package Support provides everything set out in the table at Paragraph 10.4.1 as well as direct access to the BT Security Operations Centre who will provide assistance as required and will provide support 24x7x365.

10.7 MS3 Package Support builds on the MS2 Package Support set out in Paragraph 10.6 adding a monthly TAM review. For any P1 or P2 Incident or Security Incident under the MS3 Package Support, you must have a dedicated employee who is available by phone with the necessary access to assist in troubleshooting. If an employee is not available, you will agree with BT on a timeframe for updates.

Part D – Defined Terms

11. Defined Terms

In addition to the defined terms in the General Terms and Schedule, capitalised terms in this Annex will have the meanings below (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.

"**BT Managed CrowdStrike Falcon XDR® Service**" or "**BT CrowdStrike Service**" has the meaning given in Paragraph 1.

"**CrowdStrike Licence Pack**" has the meaning set out in Paragraph 2.1.

"**CrowdStrike Falcon Portal**" has the meaning given in Paragraph 2.2.

"**Customer Security Policy**" or "**CSP**" means your security policy containing the security rules, set and owned by you, that are applied to the Managed CrowdStrike Falcon XDR® Service and determine the operation of the Managed CrowdStrike Falcon XDR® Service.

"**Change Management Process**" means the simple service request service as set out in Paragraph 2.14 of the Schedule.

"**CrowdStrike Falcon Platform**" means a software as a service platform that processes the security telemetry from the Falcon Sensor Software in line with the CrowdStrike Security Modules allowing you to protect the selected Devices and infrastructure.

"**CrowdStrike Falcon Sensor Software**" means a Supplier Software used during the licence period as set out in the Order, to be downloaded and installed on the required endpoints for the use of the CrowdStrike Falcon Platform.

"**Device**" means any mobile handset, laptop, tablet, server or other item of equipment, including all peripherals, excluding SIM Cards and applications, which are in scope of the Managed CrowdStrike Falcon XDR® Service, as set out in the Order.

"**Eagle-i**" a BT-developed security orchestration automation and remediation (SOAR) platform for false positive reduction, threat intelligence enrichment and automated quarantine of at-risk endpoint devices.

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

"**EULA**" has the meaning given in Paragraph 7.2.1.

"**Falcon Additional Data Retention"** means a service used for scalable, cloud-native data retention of third-party data within the CrowdStrike Falcon Platform.

"**Falcon Agent**" has the meaning given in Paragraph 2.6.

"**Falcon Cloud Security**" means a service that provides cloud-native application protection platform consisting of cloud security posture management and cloud workload protection.

"**Falcon Data Ingestion**" means the volume of data, measured gigabytes per day, ingested from Third-Party Security Solutions into the CrowdStrike Falcon Platform.

"**Falcon Device Control**" means a service that provides visibility and control over USB Devices in your environment.

"**Falcon Discover**" means a service that accesses your Device environment and provides you with details on unauthorised systems and applications used in your environment. It also monitors the use of any privileged User accounts in your environment.

"**Falcon Firewall Management**" means a service that simplifies host firewall policy enforcement across hosts. It eliminates the complexity of managing native firewalls by providing centralised visibility and control of firewall policies across all hosts with the Falcon Agent installed.

"**Falcon for Mobile**" means a service that provides mobile threat defence for supervised and unsupervised iOS and Android mobile fleets, with privacy controls and functionalities that protect sensitive data and minimize local resource consumption.

"**Falcon Identity Threat Protection**" means a service that provides protection against identity-based breaches in real time.

"**Falcon Insight**" means a service that provides you with detection and response capabilities to allow for continuous visibility of your endpoints.

"**Falcon Intelligence**" or "**Falcon Intel**" means a service that provides you with an automated threat analysis of your environment which will be specifically tailored to your Devices. You can raise any queries and submit malware samples for investigation by BT.

"**Falcon Overwatch**" means a service where the Supplier's threat hunting teams will proactively hunt for threats and attacks 24x7x365. If any malicious activity is identified in your environment, an Overwatch alert will be created and investigated by BT.

"**Falcon Prevent**" means a service that protects your Devices by providing anti-virus capabilities for remediating malware, exploits, malware-free and script-based attacks and stopping ransomware and known and unknown malware.

"**Falcon Search Retention**" or **"FSR"** means a service used for scalable, cloud-native data retention of third-party data within the CrowdStrike Falcon Platform.
"**General Terms**" means the general terms to which this Annex is attached or can be found at www.bt.com/terms, and that form part of the Contract.
"**Local Area Network**" or "**LAN**" means the infrastructure that enables the ability to transfer IP services within Site(s) (including data, voice and video conferencing services).
"**Minimum Period of Service**" means a period of 12 consecutive months, or the CrowdStrike Licence Pack period as set out in any applicable Order, beginning on the Service Start Date.
"**Mitigating Action**" means action taken in accordance with Paragraph 2.4 to minimise the damage of a cyber security threat.
"**Incident Mitigation**" means the mitigating action that the BT Security Operations Centre takes to minimise the damage of a cyber security threat.
"**Notice of Renewal**" has the meaning given in Paragraph 7.5.8.
"**Notice to Amend**" has the meaning given in Paragraph 7.5.7.
"**Priority**" means Priority 1, Priority 2 or Priority 3.
"**Priority 1**" or "**P1**" has the meaning given to it in the table set out at Paragraph 10.4.1.
"**Priority 2**" or "**P2**" has the meaning given to it in the table set out at Paragraph 10.4.1.
"**Priority 3**" or "**P3**" has the meaning given to it in the table set out at Paragraph 10.4.1.
"**Professional Services**" means those services provided by BT which are labour related services.
"Recurring Charges" means the Charges for the Managed CrowdStrike Falcon XDR® Service or applicable part of the Managed CrowdStrike Falcon XDR® Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Renewal Period**" means for each Managed CrowdStrike Falcon XDR® Service, the initial 12-month period following the Minimum Period of Service, and each subsequent 12-month period.
"**Schedule**" means the Managed Service Schedule to the General Terms.
"**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.
"**Third-Party Security Solutions**" means your own or other third-party security solutions that send alerts, logs and/or other data that is used in enhancing the detection and response capabilities of the Managed CrowdStrike Falcon XDR® Service.
"**Threat Analytics Manager**" or "**TAM**" means the security manager appointed by BT who will work with you in respect of the activities as set out in Paragraph 7.3 and elsewhere in this Annex.
"**Security Portal**" means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the Managed CrowdStrike Falcon XDR® Service.
"**Service Care Levels**" means the times to respond to an Incident or Security Incident that BT will endeavour to achieve in response to a fault report as set out in Paragraph 10.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**SOC**" means security operations centre.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Supplier**" means CrowdStrike Holdings, Inc. and/or CrowdStrike Services, Inc whose registered office is at 150 Mathilde Place, Suite 3000, Sunnyvale, California, United States.
"**Threat Graph**" means a feature that stores Falcon data in order to predict and prevent modern threats in real time through the use of endpoint telemetry, threat intelligence and AI-powered analytics.
"**Threat Hunting**" means the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.