



# Mobile Data Secure Management (Jamf) Annex to the BT One Phone SME Schedule

## Contents

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



## 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 Mobile Data Secure Management (Jamf)

### 1 Service Summary

BT will provide you with a mobile data security and management Service Software to control your mobile data usage, protect your business information and secure Users' Devices from Internet threats, comprising the Standard Service Components up to the point of the Service Management Boundary as set out in Paragraph 3 ("**Mobile Data Secure Management (Jamf) 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 **Service Software:** BT will provide you with access to the Service Software for the number of Devices that you purchase licences for as set out in any applicable Order.
- 2.2 When placing an Order for the Service Software, you may choose from the following three licensing options (each a "**Licensing Option**"):
  - 2.2.1 **Jamf Data Policy:**
    - (a) provides you with real time visibility of data usage by:
      - (i) volume app/site (Samsung and iOS devices only);
      - (ii) users, including groups;
      - (iii) country and use;
      - (iv) time of day, day and month; and
      - (v) business and personal use;
    - (b) Further Jamf Data Policy controls can be put in place as detailed in any applicable Order such as:
      - (i) usage controls;
      - (ii) alerts;
      - (iii) data compression; and
      - (iv) data capping;
    - (c) Jamf Data Policy controls can be managed separately for domestic and roaming usage and policies can be defined by app and by website as detailed in any applicable Order.
    - (d) Jamf Data Policy controls policies are assigned to different groups of Users that can be switched between control policies as detailed in any applicable Order.
    - (e) You can configure multiple local data plans and cost rates across different carriers in each country.
    - (f) The Jamf Data Policy Licensing Option may also leverage various techniques such as optimised browser rendering to offer Users an enhanced mobile browsing experience. These additional features as detailed in any applicable Order include:
      - (i) restricting access to certain categories, such as gambling or for specific domains, meaning you can define and limit personal usage according to your company policy;
      - (ii) defining whether the Device can be used for tethering;
      - (iii) applying different policies for data usage in your home country or when overseas;
      - (iv) deploying usage caps to prevent bill shocks;
      - (v) white-listing business applications to ensure Users remain productive even when they've reached their data cap;
      - (vi) creating custom notifications when certain thresholds are reached to alert Users how much data they've used;
      - (vii) compressing data in real-time; and
      - (viii) configuring data compression to adjust the level of data compression and data loss, including the ability to disable compression.

2.2.2 **Jamf Threat Defense:** consists of:

- (a) protection against mobile threats;
- (b) secure access layer;
- (c) vulnerability assessment;
- (d) Threat Defence.

2.2.3 **Jamf Security Suite (Jamf Data Policy & Jamf Threat Defense):** This Licensing Option consists of all capabilities provided in the Jamf Data Policy and Jamf Threat Defense. It also includes Content filtering for cellular and Wi-Fi but removes the ability to provide a secure access layer.

2.2.4 Summary of Licensing Options' services:

Services	Jamf Data Policy	Jamf Threat Defense	Jamf Security Suite
Management Portal	Yes	Yes	Yes
Mobile App	Yes	Yes	Yes
Site/App blocking	Yes	No	Yes
Tethering controls	Yes	No	Yes
Data capping	Yes	Yes	Yes
Endpoint security	No	Yes	Yes
Network security	No	Yes	Yes
EMM Connect	Yes	Yes	Yes
Customisable data retention	No	Yes	Yes
Wi-Fi Data Management	No	No	Yes
Secure Access Layer	No	Yes	No

### 2.3 RADAR Portal

2.3.1 BT will provide you with access to a web-based management portal that you may use to create and manage Service Software deployment, policies and settings with intuitive Device administration; report Incidents notwithstanding the provisions of Paragraph 8 and other service information, incorporating a self-contained Jamf Help Centre that is accessible from the main dashboard.

2.3.2 The RADAR Portal can be accessed by your Customer Contact at <https://radar.wandera.com>.

2.3.3 The Jamf Help Centre can be accessed at <https://support.wandera.com> where your Customer Contact will log in and have access to:

- (a) log a support ticket;
- (b) release notes (weekly new feature announcements);
- (c) technical support webinars;
- (d) deployment/removal guides;
- (e) troubleshooting;
- (f) connection guides;
- (g) Supplier support which includes:-
  - (i) basic support for User queries and triage;
  - (ii) investigation and resolution of higher level incidents such as adding new devices to RADAR, exporting data from RADAR and configuration;
- (h) compatibility matrixes; and

(i) FAQs.

### 3 Service Management Boundary

- 3.1 BT will provide and manage the Mobile Data Secure Management (Jamf) Service in accordance with Parts B and C of this Schedule and as set out in any applicable Order up to the point where you present traffic to, or receive traffic from any infrastructure owned or controlled by the Supplier or BT ("**Service Management Boundary**").
- 3.2 BT will have no responsibility for the Mobile Data Secure Management (Jamf) Service outside the Service Management Boundary.
- 3.3 BT does not make any representations, whether express or implied, about whether the Mobile Data Secure Management (Jamf) Service will operate in combination with any Customer Equipment or other equipment and software. BT does not provide technical support for any third-party hardware or software.
- 3.4 Access to the Mobile Data Secure Management (Jamf) Service is dependent on the suitability of any Customer Equipment (including smart phones, tablets and other similar devices capable of connecting to the Internet) and, if applicable, your network.
- 3.5 BT will not have any liability to you or any User for any data usage or telecom charges that you may incur from any Network Operator while using the Mobile Data Secure Management (Jamf) Service.
- 3.6 BT does not make any representations, whether express or implied that the Mobile Data Secure Management (Jamf) Service will prevent or detect all threats and unauthorised actions.
- 3.7 BT will not have any responsibility for storing or backing up your or your Users' Customer Data that passes through BT's or any of its subcontractors' or suppliers' servers.

### 4 Associated Services and Third Parties

- 4.1 You will have the following services in place that will connect to the Mobile Data Management (Jamf) Service and are necessary for the Mobile Data Management (Jamf) Service to function and will ensure that these services meet the minimum technical requirements that BT specifies: :
  - 4.1.1 an Internet connection at the Site(s) at all times to be able to log in to the RADAR Portal, including providing and maintaining any Customer Equipment necessary for such connection; and
  - 4.1.2 the BT One Phone Service,  
(each an "**Enabling Service**").
- 4.2 You will pay all charges related to the provision, maintenance and use of such Enabling Services and report any incidents in relation to any of the Enabling Services directly to the supplier of that Enabling Service.
- 4.3 If BT provides you with any services other than the Mobile Data Secure Management (Jamf) 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 Professional Services

- 5.1 If specified in the Statement of Requirements, BT will provide **Mobile Device Management Professional Services for Jamf** to you on the terms of the Contract and as specified in the BT Price List.
- 5.2 Within **Mobile Device Management Professional Services for Jamf**, BT will provide you with bespoke management services through BT's accredited engineers to help you manage and administer your Mobile Data Secure Management (Jamf) Service as set out in the Statement of Requirements and the BT Price List.
- 5.3 Subject to you complying with your obligations in Paragraph 8 of this Annex and Paragraph 7 of the Schedule, BT will re-perform the relevant part of the Professional Services, if:
  - 5.3.1 any part of the Professional Services are performed by BT negligently or in breach of the provisions of this Contract; and
  - 5.3.2 BT receives your written request within six months of the completion of the Professional Services.
- 5.4 Subject to Clause 22.2 of the General Terms, re-performance in accordance with Paragraph 5.3 will be your sole remedy where BT performs the Professional Services negligently or in breach of the provisions of this Contract.

### 6 Specific Terms

- 6.1 **Minimum Period of Service**



- 6.1.1 The Mobile Data Secure Management (Jamf) Service will commence from the Mobile Data Secure Management (Jamf) Service Start Date and will run co-terminus with the Minimum Period of Service for your BT One Phone Service.
- 6.1.2 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 Mobile Data Secure Management (Jamf) Service in accordance with the Contract, BT will continue to provide the Mobile Data Secure Management (Jamf) Service and each of us will continue to perform our obligations in accordance with the Contract until one of us has given Notice to the other of an intention to terminate the Mobile Data Secure Management (Jamf) Service.
- 6.1.3 If you give Notice to BT of an intention to terminate the Mobile Data Secure Management (Jamf) Service, BT will cease delivering the Mobile Data Secure Management (Jamf) Service at the time of 23:59 on the last day of the Minimum Period of Service.
- 6.2 Termination for Convenience**
- 6.2.1 For the purposes of Clause 17 of the General Terms, either of us may, at any time after the Effective Date and without cause, terminate the Mobile Data Secure Management (Jamf) Service by giving not less than 30 days' Notice to the other.
- 6.2.2 If either of us give Notice to terminate your separate contract for the BT One Phone Service to the other, the Mobile Data Secure Management (Jamf) Service will also be terminated and Termination Charges may be payable by you in accordance with Paragraph 6.9.
- 6.3 Service Transition**
- 6.3.1 If you are transitioning your existing services to BT, you will provide any information or access BT reasonably requests at least five Business Days before the Mobile Data Secure Management (Jamf) Service Start Date, including:
- (a) an inventory list with information relating to each Device to be transitioned with relevant specifications, including:
    - (i) the User's email address;
    - (ii) Device platform and type;
    - (iii) the Network Operator for the SIM card in use in the Device;
    - (iv) the home country of each Device; and
    - (v) details of any third party providing your enterprise mobility management solution where applicable.
- 6.3.2 Any changes to the inventory provided in accordance with Paragraph 6.3.1 (a) before the Mobile Data Secure Management (Jamf) Service Start Date will be made in writing and:
- (a) may cause delay to the transition of your service or the Mobile Data Secure Management (Jamf) Service Start Date; and
  - (b) may result in a change to the Charges to reflect the revised scope of the Mobile Data Secure Management (Jamf) Service,
- and your Order will be amended accordingly.
- 6.3.3 You will provide reasonable technical support to BT before and after the Mobile Data Secure Management (Jamf) Service Start Date in order to transition your existing services to BT.
- 6.4 Licence**
- 6.4.1 BT grants you a non-exclusive, non-transferable, non-sub licensable, revocable licence to download, install and use the Service Software in object code and to make the Service Software available to your Users in order to use the Mobile Data Secure Management (Jamf) Service.
- 6.4.2 As long as you have paid all applicable Charges, BT will:
- (a) provide the Mobile Data Secure Management (Jamf) Service as detailed in any applicable Order;
  - (b) provide all updates released by the Supplier; and
  - (c) use reasonable endeavours to resolve the impact of technical problems identified that materially affect BT's delivery of the Mobile Data Secure Management (Jamf) Service.
- 6.5 Customer Data**
- 6.5.1 You or your Users will be solely responsible for the quality, accuracy, integrity, legality, appropriateness and intellectual property ownership or right to use of all Customer Data.
- 6.5.2 You grant (or will procure the grant) to BT and the Supplier a royalty-free, non-exclusive licence for the term of the Contract to use the Customer Data to the extent necessary to deliver the Mobile Data Secure Management (Jamf) Service and perform its obligations under the Contract. By submitting and sending Customer Data through the Mobile Data Secure Management (Jamf) Service, you grant BT

and its Supplier permission to process and transmit the Customer Data as necessary to deliver the Mobile Data Secure Management (Jamf) Service and perform its obligations under the Contract.

- 6.5.3 In order to deliver the Mobile Data Secure Management (Jamf) Service, BT or the Supplier may need to modify the Customer Data as necessary for technical reasons including to:
- (a) reduce image resolution;
  - (b) reduce video resolution;
  - (c) block traffic; and
  - (d) optimise text-based payloads.
- 6.5.4 The Supplier and BT will have the right to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information that you or other third party provide relating to the Mobile Data Secure Management (Jamf) Service.

## 6.6 Third Party Content

- 6.6.1 In using the Mobile Data Secure Management (Jamf) Service, you may access Content, products and services provided by third parties. Neither BT nor the Supplier controls these third parties or their links, and neither BT nor the Supplier is responsible for the Content or practices of any third party.
- 6.6.2 You will refer to the policies posted by third parties on their websites regarding privacy and other topics before you use them. If you choose to purchase any products or services from a third party, your relationship is directly with the third party. You agree that neither BT nor the Supplier is responsible or liable for any loss or damage whatsoever which you may incur from dealing with any third party.

## 6.7 Limitation of liability

- 6.7.1 You will indemnify BT against all Claims, losses, costs and liabilities brought by any third parties (including your employees, workers or contractors) against BT arising out of BT's use or modification of Customer Data in accordance with Paragraph 6.5.

## 6.8 Invoicing

- 6.8.1 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) Recurring Charges monthly in advance on the first day of the relevant month and for any period where the Mobile Data Secure Management (Jamf) Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis;
  - (b) any Termination Charges incurred in accordance with Paragraph 6.9 upon termination of the relevant Mobile Data Secure Management (Jamf) Service; and
  - (c) Charges for Professional Services, one month in arrears from the date of completion of the Professional Services.
- 6.8.2 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 the BT Service Desk 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 the number of Users which exceed the limit as set out in any applicable Order (if any) in accordance with Paragraph 8.2.12;
  - (c) Charges for commissioning the Mobile Data Secure Management (Jamf) Service in accordance with Paragraph 7.2 outside of Business Hours;
  - (d) Charges for expediting provision of the Mobile Data Secure Management (Jamf) Service at your request after BT has informed you of the Customer Committed Date; and
  - (e) any other Charges as set out in any applicable Order or as otherwise agreed between both of us.

## 6.9 Termination Charges at the end of the Contract

- 6.9.1 If you terminate the Contract, the Mobile Data Secure Management (Jamf) Service or any applicable Order for convenience in accordance with Clause 17 of the General Terms you will pay BT:
- (a) all outstanding Charges for service rendered;
  - (b) any additional amounts due under the Contract;
  - (c) any other Charges as set out in any applicable Order; and
- 6.9.2 In addition to the Charges set out at Paragraph 6.9.1, if you terminate during the Minimum Period of Service you will pay BT for any parts of the Mobile Data Secure Management (Jamf) Service that were terminated during the Minimum Period of Service, Termination Charges, as compensation, equal to 100 per cent of the Recurring Charges for the Mobile Secure Management (Jamf) Service (or the terminated parts thereof) for any remaining months of the Minimum Period of Service.

## 6.10 Service Amendment



- 6.10.1 You may request, by giving BT Notice, a change to:
- (a) an Order for the Mobile Data Secure Management (Jamf) Service (or part of an Order) at any time before the applicable Mobile Data Secure Management (Jamf) Service Start Date; or
  - (b) the Mobile Data Secure Management (Jamf) at any time after the Mobile Data Secure Management (Jamf) Service Start Date.
- 6.10.2 All change requests must be made to BT.
- 6.10.3 If you request a change in accordance with Paragraph 6.10.1, except where a change results from BT's failure to comply with its obligations under the Contract, BT will, within a reasonable time, provide you with a written estimate, including:
- (a) the likely time required to deliver the changed Mobile Data Secure Management (Jamf) Service; and
  - (b) any changes to the Charges due to the changed Mobile Data Secure Management (Jamf) Service.
- 6.10.4 BT has no obligation to proceed with any change that you request in accordance with Paragraph 6.10.1, unless and until the necessary changes to the Charges, implementation timetable and any other relevant terms of the Contract to take account of the change are agreed between both of us in writing.
- 6.10.5 If you request to upgrade your Licensing Option during the Minimum Period of Service and maintain the same volume or a higher volume of licenses, and BT agrees, you will not have to pay Termination Charges for ending your existing Licenising Option. If you request to downgrade your Licensing Option during the Minimum Period of Service, or lower your volume of licences, you will pay Termination Charges in accordance with Paragraph 6.9.2.
- 6.10.6 If BT changes the Mobile Data Secure Management (Jamf) Service prior to the Mobile Data Secure Management (jamf) Service Start Date because you have given BT incomplete or inaccurate information, BT may, acting reasonably, apply additional Charges.
- 6.11 **EULA and SLASA**
- 6.11.1 Where BT makes available Software and RADAR portal for you to use with the Mobile Data Secure Management (Jamf) Service, you will be required to enter into the **Application End User License Agreement** ("EULA") and the **Software licence and services agreement** ("SLASA") in the form set out at any web-link or other location that BT or the Supplier may notify to you, as may be amended or supplemented from time to time ("SLASA").
- 6.11.2 By accepting the terms of the EULA and SLASA, you agree to observe and comply with them for any and all use of the Mobile Data Secure Management (Jamf) Service.
- 6.11.3 In addition to Clause 15 of the General Terms, if you do not comply with the EULA or SLASA, BT may restrict or suspend the Mobile Data Secure Management (Jamf) Service upon reasonable Notice, and:
- (a) you will pay the Charges that are payable for the Mobile Data Secure Management (Jamf) Service until the Mobile Data Secure Management (Jamf) Service ends; and
  - (b) BT may charge a re-installation fee to start the Mobile Data Secure Management (Jamf) Service again.
- 6.11.4 You are responsible in accordance with the terms of the EULA and SLASA for the use of the Software and RADAR portal.
- 6.11.5 You will enter into the EULA and SLASA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA or SLASA are between you and the Supplier.
- 6.11.6 You will deal with the Supplier with respect to any loss or damage suffered by you or the Supplier under the EULA and SLASA and any loss or damage will not be enforceable against BT.
- 6.11.7 Where the EULA or SLASA are 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 or SLASA.

## Part B – Service Delivery and Management

### 7 BT's Obligations

#### 7.1 Service Delivery

Before the Mobile Data Secure Management (Jamf) Service Start Date and, where applicable, throughout the provision of the Mobile Data Secure Management (Jamf) Service, BT will provide you with contact details for the Service Desk.



## 7.2 Commissioning of the Service

Before the Mobile Data Secure Management (Jamf) Service Start Date, BT will:

- 7.2.1 send you an email with the RADAR Portal log in information; and
- 7.2.2 provide you with activation support to ensure that you have access to the RADAR Portal for configuration of the Mobile Data Secure Management (Jamf) Service;
- 7.2.3 on the date that BT and the Supplier have completed the activities in this Paragraph 7.2 confirm to you the Mobile Data Secure Management (Jamf) Service Start Date.

## 7.3 During Operation

On and from the Mobile Data Secure Management (Jamf) Service Start Date, BT:

- 7.3.1 will make the Mobile Data Secure Management (Jamf) Service available in accordance with Part C of this Contract;
- 7.3.2 respond and use reasonable endeavours to remedy an Incident reported to the Service Desk without undue delay and in accordance with Part C of the Contract;
- 7.3.3 reserves the right to suspend or terminate the Mobile Data Secure Management (Jamf) Service, and to take such defensive action as it considers necessary in the event of any Attack upon the Mobile Data Secure Management (Jamf) Service;
- 7.3.4 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least ten Business Days before any Planned Maintenance on the Mobile Data Secure Management (Jamf) Service, however, BT may inform you with less notice than normal where Maintenance is required in an emergency; and
- 7.3.5 may, in the event of a security breach affecting the Mobile Data Secure Management (Jamf) Service, require you to change any or all of your passwords.

## 8 Your Obligations

### 8.1 Service Delivery

Before the Mobile Data Secure Management (Jamf) Service Start Date and, where applicable, throughout the provision of the Mobile Data Secure Management (Jamf) Service, you will:

- 8.1.1 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;
- 8.1.2 provide BT with any information reasonably required without undue delay;
- 8.1.3 complete any preparation activities that BT may request to enable you to receive the Mobile Data Secure Management (Jamf) Service promptly and in accordance with any reasonable timescales;
- 8.1.4 in jurisdictions where an employer (or any other person who receives the Mobile Data Secure Management (Jamf) Service) is legally required to make a disclosure to its employees and Users:
  - (a) inform your employees and Users that as part of the Mobile Data Secure Management (Jamf) Service being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;
  - (b) ensure that your employees and Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required); and
  - (c) agree that BT will not be liable for any failure by you to comply with this Paragraph 8.1.4, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 8.1.4.
- 8.1.5 ensure that, if legally required, labour unions or other internal or external authorities, whose consent or authorisation are required by local law, have consented and have authorised such monitoring and reporting;
- 8.1.6 be solely responsible for ensuring compliance with any Applicable Law regarding the use of the Mobile Data Secure Management (Jamf) Service in relation to any monitoring of your employees and Users, including all legal and regulatory requirements, whether based in privacy, employment, labour or consumer protection; and
- 8.1.7 be responsible for the configuration and relevant technical infrastructure required to direct traffic through the Mobile Data Secure Management (Jamf) Service.
- 8.1.8 appoint a representative for the Mobile Data Secure Management (Jamf) Service and will notify details of the representative to BT in writing on or before the Service Start Date with any changes promptly notified in writing to BT;



- 8.1.9 complete any preparation activities that BT may request to enable you to receive the Mobile Data Secure Management (Jamf) Service promptly and in accordance with any reasonable timescales;
- 8.1.10 be responsible for the configuration and relevant technical infrastructure required to direct traffic through Mobile Data Secure Management (Jamf) Service;
- 8.1.11 distribute, manage and maintain access profiles, passwords and other system administration information relating to the control of Users' access to the Mobile Data Secure Management (Jamf) Service;
- 8.1.12 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with Mobile Data Secure Management (Jamf) 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 Mobile Data Secure Management (Jamf) 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 Mobile Data Secure Management (Jamf) Service if BT requests you to do so in order to ensure the security or integrity of Mobile Data Secure Management (Jamf) Service.
- 8.1.13 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 Mobile Data Secure Management (Jamf) Service;
- 8.1.14 comply and ensure that your Users comply with all Applicable Laws, terms of use or other policies and codes applicable to use of the internet or the service provided by any Network Operator;
- 8.1.15 obtain all the necessary consents from your Users for BT to be able to provide the Mobile Data Secure Management (Jamf) Service; and
- 8.1.16 provide log files, configuration files, error messages and any other information that is required to understand and resolve any Incident.

## 8.2 During Operation

On and from the Service Start Date, you will:

- 8.2.1 ensure that Users report Incidents to the Customer Contact and not to the Service Desk;
- 8.2.2 ensure that the Customer Contact will take Incident reports from Users and report them in accordance with Paragraph 9 and is available for all subsequent Incident management communications;
- 8.2.3 monitor and maintain any Customer Equipment connected to the Mobile Data Secure Management (Jamf) Service or used in connection with a Mobile Data Secure Management (Jamf) Service;
- 8.2.4 ensure that any Customer Equipment that is connected to the Mobile Data Secure Management (Jamf) Service or that you use, directly or indirectly, in relation to the Mobile Data Secure Management (Jamf) Service is:
  - (a) adequately protected against viruses and other breaches of security;
  - (b) technically compatible with the Mobile Data Secure Management (Jamf) Service and will not harm or damage BT Equipment, the BT Network, 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;
- 8.2.5 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;
- 8.2.6 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Mobile Data Secure Management (Jamf) Service;
- 8.2.7 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;
- 8.2.8 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Mobile Data Secure Management (Jamf) 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 Mobile Data Secure Management (Jamf) 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 Mobile Data Secure Management (Jamf) Service if BT requests you to do so in order to ensure the security or integrity of the Mobile Data Secure Management (Jamf) Service.
- 8.2.9 ensure that the maximum number of Users will not exceed the permitted number, if any, of User identities as set out in any applicable Order;
- 8.2.10 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 Mobile Data Secure Management (Jamf) Service;
- 8.2.11 comply and ensure that your Users comply with all Applicable Laws, terms of use or other policies and codes applicable to use of the Internet or the service provided by any Network Operator;
- 8.2.12 inform BT within five Business Days if the number of Users increases from the number of Users as set out in any applicable Order, should any limit be agreed, and, in these circumstances, or if BT can demonstrate by management reports that the number of Users exceeds that limit, if any, BT may increase the Charges proportionately and the new Charges will apply for the remainder of the Minimum Period of Service;
- 8.2.13 obtain all the necessary consents from your Users for BT to be able to perform the Mobile Data Secure Management (Jamf) Service; and
- 8.2.14 provide log files, configuration files, error messages and any other information that is required to understand and resolve any Incident.

### 9 Notification of Incidents

Where you become aware of an Incident:

- 9.1 your Users will report it to the BT One Phone Helpdesk or via the BT One Phone Portal or use a RADAR Portal as described in Paragraph 2.3;
- 9.2 In case of Incident reporting through BT One Phone Helpdesk or via the BT One Phone Portal, BT will give you a Ticket;
- 9.3 BT will inform you when it believes the Incident is cleared and will close the Ticket when:
- 9.3.1 you confirm that the Incident is cleared within 24 hours after having been informed; or
  - 9.3.2 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.
- 9.4 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.
- 9.5 Where BT becomes aware of an Incident, Paragraphs 9.2, 9.3 and 9.4 will apply.
- 9.6 Where you report an Incident on the Mobile Network, and upon initial fault diagnosis by BT, those faults that in BT's opinion are not attributable to the Mobile Network will be referred back to the person who reported the fault.

## Part C – Service Levels

The Service Levels set out in Part C (Service Levels) of the Schedule apply to the Mobile Data Secure Management (Jamf) 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. This is to make it easier for you to find the definitions when reading this Annex.

**"Attack"** means a deliberate third party action that significantly affects the Mobile Data Secure Management (Jamf), e.g. a Distributed Denial of Service (DDoS) attack.

“**Mobile Data Secure Management (Jamf)**” has the meaning given in Paragraph 1.

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

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

“**Customer Contact**” means any individual authorised to act on your behalf for Mobile Data Secure Management (Jamf) management matters.

“**Customer Data**” means all data, including all text, sound, or image files and software provided to BT or BT’s licensors (or both) by you or on your behalf through your use of the Mobile Data Secure Management (Jamf), and may include Personal Data.

“**Customer Equipment**” means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a Mobile Data Secure Management (Jamf).

“**Jamf Data Policy**” means the Software licence option that will provide you with real time visibility of Users’ data usage on their Devices and as more particularly described in Paragraph 2.2.1

“**Jamf Security Suite (Jamf Data Policy & Jamf Threat Defense)**” means the Software licence option that will provide you with real time visibility of Users’ data usage on their Devices and protection against mobile threats as described in Paragraph 2.2.3

“**Device**” means the devices provided with your BT One Phone Service, excluding SIM Cards and applications, which are in scope of the Mobile Data Secure Management (Jamf) Service, as set out in the Order.

“**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](http://www.bt.com/terms), and form part of the Contract.

“**Incident**” means an unplanned interruption to, or a reduction in the quality of, the Mobile Data Secure Management (Jamf) or particular element of the Mobile Data Secure Management (Jamf).

“**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.

“**Minimum Period of Service**” means a period of consecutive months as set out in the Order beginning on the Mobile Data Secure Management (Jamf) Service Start Date.

“**Mobile Device Management Professional Services for Jamf**” – has the meaning given in Paragraph 5.2

“**Jamf Threat Defense**” means the Software licence that will provide you with protection against mobile threats and as more particularly described in Paragraph 2.2.2.

“**Network Operator**” means any mobile communications system network operator which provides wireless or mobile voice and data services to you or your Users.

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

“**Professional Services**” means the services specified in the Statement of Requirements.

“**RADAR Portal**” has the meaning given in Paragraph 2.3.

“**Recurring Charges**” means the Charges for the Mobile Data Secure Management (Jamf) or applicable part of the Mobile Data Secure Management (Jamf) that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.

“**Schedule**” means the BT One Phone SME Schedule.

“**Service Desk**” means means the BT One Phone helpdesk that you are able to contact to submit service requests, as well as notwithstanding the provisions of Paragraph 2.3 to report Incidents and ask questions about the Mobile Data Secure Management (Jamf) Service.

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

“**Service Software**” means the Supplier’s cloud based Jamf software.

“**SLASA**” has the meaning given in Paragraph 6.11

“**Site**” means a location at which the Mobile Data Secure Management (Jamf) is provided.

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

“**Statement of Requirements**” means BT’s form that may be used to detail your requirements in relation to your particular Mobile Data Secure Management (Jamf) Service.

“**Supplier**” means Wandera Limited, with company number 07998183 and registered address (office) at 45 Mortimer Street, London, W1W 8HJ.

“**Threat Defence**” means a Service Software functionality which provides you with protection against a broad spectrum of mobile threats, through real-time detection, and a score-based risk assessment of apps, sites, Devices and overall company health rating.

“**Ticket**” means the unique reference number provided by BT for an Incident reported in accordance with Paragraph **Error! Reference source not found.** and that may also be known as a fault reference number.

“**Jamf Help Centre**” means the Supplier’s Help Centre accessed through the RADAR Portal.

“**WiFi**” means wireless local area network products that are based on the Institute of Electrical and Electronics Engineers’ (IEEE) 802.11 standards.