


Resilience

Schedule to the General Terms

Contents

1. General
 2. ISDN Dial Around
 3. ISDN Dial Back Up
 4. Managed Express Recovery
 5. Managed Dynamic Recovery
 6. ADSL Managed Resilience
 7. Blue Coat Resilience
 8. Firewall Resilience
 9. IPS Resilience
 10. IP Converge Disaster Recovery
 11. 3G/GPRS Back Up Service
 12. IP Converge Auto Fallback Service
 13. Defined Terms
- 

Resilience

Where the Customer selects an option from Resilience as detailed in the Order, the following additional conditions shall apply:

1. General

- 1.1. Except as set out in paragraph 2.3 of this Service Schedule, the Customer will ensure that any Line provided as part of a resilience option will not be used other than in circumstances in which the circuit primarily used to provide Service to the Site is faulty. The Customer will use any on line monitoring facility provided by BT solely for the purpose of monitoring the Service.
 - 1.1.1. Where BT is providing a back-up circuit and a primary circuit at the same time or as part of the same Order the Customer will permit BT to test the back-up circuit after the primary circuit has been installed, in order to ensure it works correctly. The Customer accepts that such testing may result in a temporary loss of Service and the Customer may be required to physically power down the primary circuit while testing is taking place. For the avoidance of doubt any applicable Service Level options will not apply until successful testing has taken place.
 - 1.1.2. In the event that the Customer does not permit BT to test the back-up circuit BT will not be liable for failure of the back-up circuit. In such circumstances, the Customer will be deemed to have failed to observe their obligations under this paragraph and BT will have no liability to the Customer relating to the provision of the Service, the performance of the Service or its effect on other Services or CPE. For the avoidance of doubt any applicable Service Level options will not apply until successful testing has taken place.
 - 1.1.3. The testing of a back-up circuit must take place within a reasonable period from installation of the back-up circuit and the Customer accepts and acknowledges that any applicable Service Levels will not apply until successful testing has taken place.
- 1.2. Where BT is providing a back-up circuit to an existing primary circuit the Customer will permit BT to test the back-up circuit within a reasonable period from installation of the back-up circuit. As set out in paragraph 1.1.1 above, such testing may result in a temporary loss of Service and a requirement to power down the primary circuit. In the event that the Customer does not permit such testing BT will not be liable for failure of the back-up circuit, and will have no liability to the Customer relating to the provision of the Service, the performance of the Service or its effect on other Services or CPE. The Customer accepts and acknowledges that any applicable Service Levels will not apply until successful testing has taken place.
- 1.3. Where the Customer has selected a Service where BT is providing a primary circuit and a secondary back-up circuit these will be treated as the provision of two separate circuits and will be invoiced respectively in accordance with the General Terms. For the avoidance of doubt BT shall be entitled to invoice for the primary circuit from the CDD of that circuit regardless of whether the secondary back-up circuit has been installed and vice versa.

2. ISDN Dial Around

- 2.1. BT will provide an appropriate ISDN connection at each Site, including any necessary ancillary circuit termination equipment.
- 2.2. BT will test the connection provided as part of the ISDN Dial Around resilience option at least once a day using a non-intrusive method and shall take all appropriate steps to rectify any identified problems as soon as reasonably practicable.

2.3. Where ISDN Dial Around - Call Charges Exclusive has been selected, circuit rental and usage Charges are levied separately. If the Customer chooses this option, the restriction on use of the ISDN Dial Around circuits contained in paragraph 1.1 of this Service Schedule will not apply.

2.4. Where ISDN Dial Around - Call Charges Inclusive has been selected, all usage Charges in relation to the ISDN Dial Around circuits are covered in the rental charge. In this case, usage Charges will not apply in cases where the ISDN circuits are used because the circuits primarily used to provide the Service are faulty. However, usage Charges will be levied where such ISDN circuits are used other than for backup purposes.

3. ISDN Dial Back Up

3.1. BT will provide an ISDN Backup unit at the Site and at the node of the BT Network. BT will also provide appropriate ISDN connections, except at Sites located outside the UK at which it shall be the Customer's responsibility to arrange for the provision of the necessary circuits by the relevant local telecommunications service provider.

3.2. Where ISDN circuits are provided as part of the ISDN Dial Backup resilience option, usage Charges will not apply in cases where the ISDN circuits are used because the primary circuits used to provide the Service are faulty. However, usage Charges will be levied where such ISDN circuits are used other than for backup purposes.

4. Managed Express Recovery

4.1. This Service element provides rapid provision or re-grading of Cell and Cellframe PVCs from the Customer's primary host to the Customer's disaster recovery host Site in the event of a catastrophic failure of the host environment.

4.2. The managed Express Recovery Service is only available for Cellstream PVCs and the Cell end of Cell-Frame PVCs.

4.3. A separate Express Recovery plan is required for each scenario and each is priced separately. Where a test plan is required which uses a subset of the PVCs included in the main plan this is priced independently of the main plans.

4.4. An invocation charge is payable upon invocation of the plan, however two tests per year are included within the Service pricing where the test is planned at least twenty-eight days in advance.

4.5. Up to 200 PVCs can be included in any one main plan.

4.6. Multiple plans per Customer are available.

4.7. Where multiple Customers request invocation of multiple plans simultaneously, requests will normally be dealt with on first come, first served basis, however priority will always be given to Emergency services and health service customers.

4.8. BT will endeavour to complete invocation within four hours of reporting the request to the helpdesk for a single plan. Multiple plans will be invoked on a pro-rata basis.

5. Managed Dynamic Recovery

5.1. This Service element will provide a Service using shadow (or Backup) PVCs between each of the branches to a dedicated Host Disaster Recovery Site.

5.2. The Managed Dynamic Recovery Service is only available for CellStream PVCs, Cell-Frame PVCs.

- 5.3. Routing algorithms implemented using standard dynamic routing protocols (RIP, OSPF, IGRP, and BGP etc.) will direct all of the Customer's traffic between each branch and the Customer's main host during normal operation. Under a failure scenario all PVCs will dynamically re-converge on to the Customer's Disaster Recovery host router in the event of a major failure within the Customer's main host environment.
- 5.4. The Customer's host routers will be re-configured where appropriate.
- 5.5. Checks will be performed to ensure that each of the Customer's branch sites have successfully been restored in the event of invocation.
- 5.6. The Customer may be required to physically power down the main host in order to effect invocation in the event that the main host router remains unaffected by the disaster.
- 5.7. A maximum of two tests per year of the Service can be performed (separate test plans will be charged separately). All tests must be requested by the Customer.
- 5.8. Partial or full testing can be carried out for this Service element, however where a partial test is performed the scope of this test will be limited by the routing methodology.
- 5.9. The Customer may also request that BT effects manual invocation.

6. ADSL Managed Resilience

- 6.1. The Service is offered as a bundled Service which offers network access and pre-defined CPE, terminating on a managed router. The Service also includes as standard, Project Management with BT Desk Based Project Manager, Standard Care Maintenance, and Rapid Fault Diagnostics or Standard or Enhanced Incident Management.
- 6.2. The ADSL Managed Resilience Service is for resilience only, the Service should not be used to carry data traffic. Where the Customer requires a Service to carry data traffic the ADSL Managed Service should be used.
- 6.3. The Customer must provide BT with their IP addresses. The Service will not be available outside the Service Availability Area, and availability within the Service Availability Area will be subject to the provisions of this paragraph 6. Provision of the Service may be subject to a Site survey and as a result BT may not be able to provide the Service.
- 6.4. The Customer NTE (excluding any Ethernet cable which may also be provided) requires local mains power directly from a wall mounted socket, or an appropriately approved mains extension lead which is the responsibility of the Customer to provide.
- 6.5. Without prejudice to BT's obligations under this Contract, the Customer accepts and acknowledges that BT has the right to use the physical network component (including the Metallic Pair) to provide other services, this will be at the Customer's request and BT's discretion.
- 6.6. The Customer acknowledges and accepts that provision of the Service may result in the Customer experiencing a temporary loss of analogue direct exchange line service whilst activation is being carried out, and that any incorrectly wired extensions to existing master sockets forming part of the BT Network will be left disconnected.
- 6.7. BT reserves the right to cancel any order where the Customer has failed to agree with BT an activation date within thirty days from acceptance by BT. If BT cancels an Order request in accordance with this paragraph 6.7, then the Customer must pay applicable cancellation Charges specified by BT.

- 6.8. The Customer acknowledges and accepts that there may be some technical limitations within the BT Network that may not become apparent until after the Service has been installed. In such circumstances, the Service may need to be withdrawn in which case BT will refund any Charges paid in advance by the Customer.
- 6.9. In the circumstances referred to in paragraphs 6.3 and 6.8 above, except in respect of a refund referred to in paragraph 6.8, BT will have no liability to the Customer relating to the provision of the Service (or BT's inability to provide the Service), the performance of the Service, its effect on other services or equipment or the withdrawal of the Service.
- 6.10. The Customer must have a contract for the use of a BT provided analogue direct exchange line which terminates on a BT public switched telephone network master socket forming part of the BT Network for the duration of the Contract.
- 6.11. In the event that BT re-locates a DSLAM it is possible that some ADSL Services will cease to be operational as a result of increased distance between the re-located DSLAM and the BT Equipment. In these circumstances, the Service will be withdrawn in which case BT will refund any Charges paid in advance by the Customer on a pro rata basis. BT will give the Customer as much notice as reasonably possible of any such re-location of a DSLAM.

7. Blue Coat Resilience

- 7.1. Blue Coat Failover - This Service provides two instances of the Blacklisting and/or Antivirus service at a single Customer Site. Duplicate hardware and Software is provided and both instances are connected via a single connecting switch to a de-militarised zone on the associated firewall. In the case of Blacklisting, if one instance fails, the other will take over. In the case of the Antivirus Service both instances share the load unless one fails, if this occurs then the other takes over the full load.
- 7.2. Blue Coat High Availability - This Service provides two instances of the Blacklisting and/or Antivirus service at a single Customer Site. Duplicate hardware and Software is provided and both instances are connected, via a resilient pair of connecting switches, to de-militarised zones on the associated resilient firewalls. In the case of Blacklisting, if one instance fails, the other will take over. In the case of the Antivirus Service both instances share the load unless one fails, if this occurs then the other takes over the full load.
- 7.3. Blue Coat Dual Site Resilience - This Service provides resilience across two Customer critical Sites. In the event of a catastrophic failure at either Site, the Service will continue (or can be recovered) at the alternative Site. The Dual Site Resilience Service (DSR) is only available in association with resilient firewalls and resilient Internet access. The Dual Site Resilience Service can be provided where both Customer Sites are configured to either the Failover Service or the High Availability Service as described above. In the event of one Customer Site failing, the Internet traffic will be re-routed to the other Site. The Customer must specify if this is to occur automatically or manually. If the Customer requests a single Anti-Virus server at each Site, a high speed interconnection is required between the primary and secondary Customer Sites.

8. Firewall Resilience

8.1. Firewall Failover

Firewall Failover resilience involves a "hot standby" Service, which takes over if the main firewall Service fails. The hot standby Service continuously holds data on the state of connections that are open on the main firewall Service, which enables a smooth transition for Users in the event of failover.

8.2. Firewall High Availability

High Availability or Load-sharing Firewalls are continuously in operation, with traffic shared between them by the surrounding network infrastructure. If one firewall fails, the solution will route all subsequent traffic to the remaining firewall.

9. IPS Resilience

9.1. IPS Failover

This Service provides two IPS sensors at a single Customer Site. Identical hardware, Software and policy configurations are required on both sensors. The Service provides one sensor which is the “Active” sensor while the other is the “Secondary” sensor. The active sensor performs normal network functions while the secondary sensor monitors, ready to take control should the active sensor fail. Failover sensors maintain synchronised state information at all times. The IPS sensors are invisible to the network around them and therefore are not capable of routing. A Failover IPS solution needs to work in conjunction with a Failover Firewall and/or surrounding network design.

9.2. IPS High Availability

This Service provides two IPS sensors at a single Customer Site. Identical hardware, Software and policy configurations are required on both sensors. Both sensors can monitor the traffic flow and are capable of asymmetric routing. If one sensor fails then the other sensor can monitor all traffic. The IPS sensors are invisible to the network around them and therefore are not capable of routing. IPS High Availability needs to work in conjunction with a High Availability Firewall and/or surrounding network design.

9.3. IPS Dual Site Resilience

This Service provides resilience across two Customer critical Sites. In the event of a catastrophic failure at either Site, the Service will continue (or can be recovered) at the alternative Site. The Dual Site Resilience Service (DSR) is only available in association with resilient BT managed firewalls and resilient internet access. The IPS Dual Site Resilience Service can be provided where both Customer Sites are configured to either the IPS Failover Service or the IPS High Availability Service. In the event of one Customer Site failing, the Internet traffic will be re-routed to the other Site. The Customer must specify if this is to occur automatically or manually. Depending on solution design the Customer may require a high speed interconnection between the primary and secondary Customer Sites. IPS sensors are invisible to the network around them and therefore are not capable routing.

10. IP Converge Disaster Recovery

10.1. As part of this Service element, BT will provide a disaster recovery Service which gives the Customer the ability to manually invoke a pre-agreed disaster recovery plan, transferring Service from the Customer's host Site to the disaster recovery Site in the event of a major failure at the Customer's Host Site.

10.2. A disaster recovery plan can only be implemented for a host Site. The disaster recovery plan will be produced by BT and will include a description of what warrants a major failure, a pre-defined list of Services that will be transferred from the Customer host Site to the disaster recovery Site in the event of a major failure at the host Site, and the process for invoking the disaster recovery plan. The Customer will provide BT with assistance in the preparation of the disaster recovery plan.

10.3. The Customer is responsible for invoking the disaster recovery plan. The Customer must provide BT with a list of Customer contacts that are authorised to invoke the disaster recovery plan. The Customer is also responsible for informing BT when Services should be restored back to the Customer host Site.

- 10.4. The disaster recovery Site will have an identical access type, bandwidth, LAN interfaces and IP addressing, to the Customer host Site.
- 10.5. When not in use, the disaster recovery Site is dormant and will not be accessible to the Customer. Upon invocation of the disaster recovery plan the Customer host Site will be disabled and the disaster recovery Site will be activated. Any sessions active during the transition from the Customer host Site to the disaster recovery Site will be lost and the Customer will be responsible for providing all necessary services to support its Users.
- 10.6. Checks will be performed by BT to ensure that each of the Customers' branch sites have successfully been restored in the event of invocation.
- 10.7. A Charge is payable upon each and every request from the Customer to invoke the disaster recovery plan.
- 10.8. One test per year is included within the Service pricing where the test is planned at least twenty eight days in advance (separate test plans will be charged separately). All tests must be requested by the Customer. The Customer acknowledges and accepts that testing will be Service affecting.
- 10.9. BT will aim to complete invocation of the disaster recovery plan within 24 hours of receiving and validating a request from the Customer.
- 10.10. Service level agreements are not available with this Service. Any indicated levels of performance are targets and the Customer acknowledges and agrees that BT shall not be liable for failure to meet any such targets.

11. 3G/GPRS Back Up Service

11.1. Service Overview

- 11.1.1. This Service is a resilience Service for branch Sites available to Customers with IP Clear and/or ADSL managed networks. It enables data to be transferred over the BT Mobile Network to the Customer's host Site in the event of a failure at the Customer's branch Site(s).
- 11.1.2. The Service includes as standard Project Management with BT Desk Based Project Manager, Rapid Diagnostics or Standard ADSL Incident Management and 3G/GPRS Mobile Operator Support.
- 11.1.3. The Service also includes the following BT Purchased Equipment; a 3G/GPRS card and a SIM Card. BT will provide, install, configure and support the 3G/GPRS card and SIM Card in the remote branch Site router. The 3G/GPRS card is supplied with an integral antenna, an external antenna can be supplied by BT for an additional charge. The 3G/GPRS Card is maintained under a CPE maintenance option as selected in the Order.
- 11.1.4. The following Services are also available at an additional charge: 3G/GPRS Enhanced Mobile Operator Support, 3G/GPRS Standard reports, 3G/GPRS Customer Service Manager and 3G/GPRS Site Coverage Check.
- 11.1.5. The Service should only be used to carry traffic as part of a back-up Service and should only be used as a resilience Service for branch Sites only. It is not designed as a host Site resilience Service. The 3G/GPRS card will be enabled to transfer data to the Customer host Site when a failure occurs at the Customer's branch Site. The Service does not allow data to be transferred between branch Sites.

- 11.1.6. The 3G/GPRS Back Up Service is delivered using the BT Mobile Network and is subject to BT Mobile Network availability. However, BT does not guarantee the availability and/or performance of the BT Mobile Network. The 3G/GPRS Back Up Service does not include any in life testing as part of the Service. BT will install the Service and carry out standard tests to ensure that the 3G/GPRS card is operational and connected to the BT Mobile Network.
- 11.1.7. The Customer acknowledges and accepts that there may be some technical limitations within the BT Mobile Network that may not become apparent until after the Service has been installed. In such circumstances, the Service for some individual Sites may need to be withdrawn in which case BT will rebate any Charges paid in advance by the Customer.
- 11.1.8. In the circumstances referred to in paragraph 11.1.7 above, BT will have no liability to the Customer relating to the provision of the Service (or BT's inability to provide the Service), the performance of the Service, its effect on other services or equipment or the withdrawal of the Service.
- 11.1.9. It is recommended that Customers enable IPSec encryption on all 3G/GPRS Back Up Services.
- 11.1.10. There are no Service Levels offered as part of the Service which cover latency, coverage, bandwidth availability or bandwidth throughput on the BT Mobile Network used to provide the Service.

11.2. Service Options

- 11.2.1. Following a failure at the Customer's branch Site(s), the Service will enable transfer of Customer data using one of three options:
- (a) 3G/GPRS Public Back Up Service which uses the public internet to deliver data from the branch Site to the host Site.
 - (b) 3G/GPRS Shared Back Up Service which uses a shared access circuit from the BT Mobile Network to a BT data centre and then onto the Internet.
 - (c) 3G/GPRS Corporate Back Up Service which uses a dedicated private circuit from the BT Mobile network to the Customers host Site. As part of this option, BT will install and maintain a dedicated private circuit from the BT Mobile Network.

BT will provide the Customer with a unique Access Point Name ("**APN**") for access to the Shared Back Up and Corporate Back Up Services. The APN is provided as standard with a 3G/GPRS data only SIM Card. As part of the 3G/GPRS Shared and Corporate Back Up Service, Radius Authentication is provided and maintained by BT.

11.3. 3G/GPRS Public Back Up Service

- 11.3.1. Under this option BT will configure the 3G/GPRS card and SIM Card to deliver the Customer's data over the BT Mobile Network to the Customer's host Site over the public Internet in the event that a failure occurs on the Primary access circuit at the Customer's branch Site. It is the Customer's responsibility to ensure that its Internet access has sufficient bandwidth to support the additional data traffic.
- 11.3.2. The Customer's Internet Firewall at the host Site must be configured to enable IPSec encryption from the remote branch Sites. In addition it is recommended that a separate and dedicated LAN area from the firewall to the host Site is provided to connect the IPSec Gateway. For an additional charge and where required BT can provide a managed firewall.

11.3.3. As part of this option BT will provide username and password verification for the 3G/GPRS Card and SIM Card, using the Radius Authentication process. Radius Authentication will be provided by BT Mobile.

11.3.4. This option is only available to Customers who have selected 3G/GPRS Mobile Operator support at all branch Sites. 3G/GPRS Enhanced Mobile Operator Support and 3G/GPRS reporting cannot be used under this option.

11.3.5. The 3G/GPRS card will be configured by BT to transmit the Customer's data over the BT Mobile Network automatically if the primary network access on the branch Site router has a major outage preventing connection to the network. The card is configured to automatically switch back to primary network connection on the branch Site router when the outage is resolved.

11.4. 3G/GPRS Shared Back Up Service

11.4.1. Under this option BT will configure the 3G/GPRS card and SIM Card to deliver the Customer's data over a shared access Private Circuit via the BT Mobile Network to a BT data centre when a fault occurs on the primary access circuit at the Customer branch Sites(s) or network. The Customer data traffic is delivered to the Customer's host Site from the BT data centre over the public Internet. It is the Customer's responsibility to ensure there is sufficient Internet bandwidth and IPSec encryption capability at the host Site.

11.4.2. The Customer's internet firewall at the host Site must be configured to enable IPSec encryption from the remote branch Sites. In addition, it is recommended that a separate and dedicated LAN area from the firewall to the host Site is provided to connect the IPSec Gateway. For an additional charge and where required BT can provide a managed firewall.

11.4.3. This option is only available to Customers that have selected 3G/GPRS Mobile Operator support at all branch Sites. As part of this option BT will provide radius authentication to enable the 3G/GPRS card and SIM Card to be connected to the BT Mobile Network.

11.4.4. BT will be responsible for the provision and support of the access from the BT Mobile Network into the BT data centre. Access from the BT data centre to the Customers host Site will be via the public Internet. BT will be responsible for the Internet access at the BT data centre.

11.4.5. The 3G/GPRS card will be configured by BT to transmit the Customer's data over the mobile network automatically if the primary network access on the branch Site router has a major outage preventing connection to the network. The card is configured to automatically switch back to primary network connection on the branch Site router when the outage is resolved.

11.5. 3G/GPRS Corporate Back Up Service

11.5.1. Under this option BT will provide a dedicated Private Circuit from the BT Mobile Network to the Customer's host Site. BT will configure the 3G/GPRS card and SIM Card at the branch Sites to deliver the Customer's data over a dedicated Private Circuit via the BT Mobile Network to the Customer's host Site when a major outage occurs on the primary network access at the Customer branch Sites(s).

11.5.2. As part of the 3G/GPRS Corporate Back Up Service BT will provide and support a terminating router at the host Site, this will be connected to the dedicated Private Circuit from the BT Mobile Network and provide a RJ45 interface to the Customer's host LAN.

11.5.3. This option is only available to Customers that have selected 3G/GPRS Mobile Operator support at all branch Sites.

11.5.4. As part of this option BT will provide radius authentication to enable the 3G/GPRS card and SIM Card to be connected to the BT Mobile Network. BT will also configure the 3G/GPRS card for IPsec data encryption.

11.5.5. The 3G/GPRS card will be configured by BT to transmit the Customer's data over the BT Mobile Network automatically if the primary network access on the branch Site router has a major outage preventing the connection to the network. The card is configured to automatically switch back to primary network connection on the branch Site router when the outage is resolved.

11.5.6. The dedicated Private Circuit is supplied at a flat rate connection and rental charge subject to the Customer host Site being within 100km of the BT Mobile POP. Where the Customer host Site is further than 100km from the BT Mobile POP additional connection and rental charges will apply. Provision of the dedicated Private Circuit is subject to survey. Standard termination charges will apply in the event that the Customer terminates the Private Circuit during the Minimum Period.

11.6. SIM Cards

11.6.1. The Service includes the supply by BT of a SIM Card which must be used for each connection to the 3G/GPRS Back Up Service. SIM cards from other Mobile Network suppliers cannot be used with the Service.

11.6.2. BT will allocate a number for use with the SIM Card. The number belongs to BT and may only be transferred to another service provider with BT consent and in accordance with prevailing industry rules and processes.

11.7. Using the Service with an IP Clear Network

11.7.1. Where the 3G/GPRS Service is used with an IP Clear network and the Host Site is served with a single IP Clear access and single access router, a gateway router will be required at an additional charge from BT. This gateway router will provide a single RJ45 FastEthernet port to the Customer's network and is the access point into the BT 3G/GPRS Service.

11.7.2. Where the 3G/GPRS service is used with an IPClear Network and the host Site is served with dual Access routers with FastEthernet connectivity there will be no requirement for a gateway router.

11.8. Using the Service with an ADSL Managed Network

11.8.1. Where the Customer's ADSL Managed network has a 2M or 155M BT Central connection the 3G/GPRS Back Up service is not available.

11.8.2. Where the Service is used with an ADSL Managed network a Gateway Router will be required between the BT Central router and Customer's access LAN. This will be provided by BT at the Customer's host Site at an additional charge.

11.9. Mobile Team Tariff

11.9.1. The Charges for the Service will be applied in accordance with the Mobile Team Tariff. The Mobile Team Tariff is a monthly rental charge based on the number of remote branch Sites included in the 3G/GPRS Back Up Service.

11.9.2. Each Mobile Team Tariff banding specifies the maximum number of branch Sites that can be included within each team tariff banding. If the Customer increases the number of branch Sites beyond the maximum applicable to that banding, the next applicable higher banding will then be applied by BT. If the Customer reduces the number of remote branch Sites on the 3G/GPRS Back Up Service below the minimum applicable to their banding, the next applicable lower banding will then be applied by BT.

11.9.3. The maximum number of remote branch Sites on Mobile Team Tariff is 700 per 3G/GPRS Back Up Solution. Networks with more than 700 remote branch Sites will require an additional team tariff. The minimum number of Sites is one.

11.9.4. The Mobile Team Tariff also includes an allowance for data transfer per month. If the Customer exceeds the maximum data transfer beyond the maximum applicable to their tariff banding BT will charge for the additional capacity used. The team tariff data allowance enables all of the inclusive data allowance to be used by a single Site or by multiple Sites within a calendar month.

11.10. Radius Authentication

11.10.1. Radius authentication is provided by BT for the 3G/GPRS Shared Back Up and 3G/GPRS Corporate Services only. Radius authentication is provided by BT Mobile for the 3G/GPRS Public Service.

11.11. Customer Responsibilities

11.11.1. The Customer is responsible for:

- (a) providing appropriate network infrastructure (Routers, Firewalls, IPsec Concentrators) that facilitate connection to the Service. The terms of this Paragraph 11.11.1(a) only apply if the Customer has not selected the BT Managed Security Service;
- (b) providing suitably qualified personnel to configure the Customer Equipment (Routers, Firewalls, VPNs etc.) in order to facilitate network access to the Service;
- (c) providing sufficient bandwidth to enable successful transmission between the Customer's network and the Internet, where this is the chosen method of connection to the Service. The terms of this paragraph 11.11.1(c) only apply where the Customer has selected the 3G/GPRS Public Back Up Service or/and 3G/GPRS Shared Back Up Service;
- (d) providing trained staff to support the use of the Service;
- (e) providing BT with their IP address and the IP address that is to be used for the configuration and set up of the network CPE.

12. IP Converge Auto Fallback Service

12.1. Service Overview

12.1.1. Under this Service option BT will provide a resilience Service which gives the Customer service continuity in event of a major failure at the Customer's Primary Site. Service is automatically transferred from the Customer's Primary Site to a Fallback Site in the event of a failure at the Customer's Primary Site.

12.1.2. This Service is a resilience Service for host or branch Sites and is only available where the Customer has an IP Converge network.

12.1.3. The Service includes two Standard Access Lines. The Service is available on fixed or flex Access Lines with bandwidths of 256k or greater. The Service is not available on ADSL Access Lines or Secure or Secure + Access Lines.

12.1.4. The Customer must nominate the Primary Site and the Fallback Site in the Order.

12.1.5. Checks will be performed by BT to ensure that each of the Customers' branch Sites have successfully been restored once Service at the Primary Site is restored.

12.1.6. The Customer acknowledges and accepts that on occasion there may be technical issues which result in the Service not automatically transferring to the Fallback Site. BT will take all reasonable steps to resolve any Service issues as soon as they become apparent, but in respect of the service issues described above BT will have no liability to the Customer for performance of the Service.

12.1.7. This resilience Service does not include any service level agreement options. Any indicated levels of performance are targets and the Customer acknowledges and agrees that BT shall not be liable for failure to meet any such targets.

12.2. Service Options

12.2.1. Single Site Fallback

- (a) Under this Service option the Primary Site and Fallback Site must be served from the same PoP.
- (b) If the primary access at the Primary Site fails service is automatically transferred to the secondary access at the Customer's Fallback Site.
- (c) The Fallback Site must have an identical access type, LAN interfaces and IP addressing as the Primary Site.
- (d) The bandwidth of the Fallback Site must be equal to or less than the bandwidth of the Primary Site.
- (e) Load sharing to utilise available bandwidth on the Secondary Access is not permitted.
- (f) While not in use the secondary access at the Fallback site is dormant and will not be accessible to the Customer. The secondary access is for standby purposes only if the primary access at the Primary Site fails.

12.2.2. Separate Site Fallback

- (a) Under this Service option the Primary Site and Fallback Site must be served from different PoPs. The PoPs must be in completely different physical locations and must not be in the same town or county as this could result in the same PoP being used. Where the use of different PoPs cannot be achieved an alternative method of resilience must be selected.
- (b) If the primary access at the Primary Site fails service is automatically transferred to the secondary access at the Customer's Fallback Site.
- (c) The Fallback Site must have identical IP addressing LAN Interfaces and Servers as the Primary Site.
- (d) The bandwidth of the Secondary Access at the Fallback Site must be equal to or less than the Primary Access at the Host Site.

- (e) Load sharing to utilise available bandwidth on the Secondary Access is not permitted.
- (f) While not in use the secondary access at the Fallback Site is dormant and will not be accessible to the Customer. The secondary access is for standby purposes only if the primary access at the Primary Site fails.

12.2.3. Combined Fallback and Outstation Access

- (a) Under this Service option the Primary Site and Fallback Site will be terminated on separate NTE routers and the circuits must be served from different PoPs. The PoPs must be in completely different physical locations and must not be in the same town or county as this could result in the same PoP being used. Where the use of different PoPs cannot be achieved an alternative method of resilience must be selected.
- (b) As part of this Service option the Fallback Site acts as a fallback for the Primary Site and simultaneously works as an active Site on the VPN.
- (c) A separate interface is provided for the fallback LAN at the Fallback Site. A second VPN connection at the Fallback Site is also required.
- (d) The bandwidth of the Secondary Access at the Fallback Site must be equal to or less than the Primary Access at the Primary Site.
- (e) Load sharing to utilise available bandwidth on the Secondary Access is not permitted.
- (f) Where possible the circuits will use separate duct paths, but this cannot be guaranteed.

13. Defined Terms

In addition to the defined terms in the General Terms and Managed Service from BT Schedule, the following defined terms apply in this Schedule (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule):

“3G” means the third-generation in the context of mobile phone standards. The services associated with 3G include wide-area wireless voice telephony and broadband wireless data, all in a mobile environment.

“APN” means the Access Point Name given to the unique point (or points) at which the Customer Network or a public network such as the Internet may connect with the Network.

“BT Central” means the physical network and protocol that connects a Customer NTE to the Broadband Access Server. Broadband Access Server means a remote access server, a component in the BT Network and which is used for the Service.

“BT Mobile Network” means the communications network BT uses to provide the Service.

“DSLAM” means digital subscriber line access multiplexer.

“Fallback Site” means the site nominated by the Customer to Secondary Access

“Firewall” means a hardware device together with any associated Software, designed to prevent unauthorised access to the Customer’s LAN.

“**GPRS**” means General Packet Radio Service for the transmission of data.

“**Primary Site**” means the site nominated by the Customer to be the Primary Access.

“**Private Circuit**” means a terrestrial telecommunication link provided between two or more specified points within the UK (none of which is a point at which BT’s telecommunications systems are connected to telecommunications systems run by another telecommunications provider), other than by means of one of BT’s public switched telecommunications systems.

“**PVC**” means a Permanent Virtual Circuit which is configured to provide a virtual path over BT’s Network between the Customer’s selected Sites.

“**RADIUS**” means Remote Authentication Dial In User Service and is the industry standard for User authentication, authorization, and accounting.

“**Service Availability Area**” means an area, as may be amended by BT from time to time, where the Service is potentially available detailed on the BT website at <http://www.bt.com/broadband/>.

“**SIM Card**” means Subscriber Identity Module and refers to the smart card within a mobile CPE device or cellular handset.

“**Standard Access**” means an access with no resilience.