Terms and Conditions

1. Definitions and Interpretation

1.1 In this Contract, including its Schedules, the following words shall, unless the context clearly requires otherwise, have the following meanings:

"BT"	means British Telecommunications plc of 81 Newgate Street, London EC1A 7AJ, registered in England No. 1800000
"Bulk Email"	means a group of more than five thousand (5000) Email messages with substantially similar content sent or received in a single operation or a series of related operations;
"Contract"	means, in order of precedence, the Conditions, the Order Form Amendment (if any), the Service Schedule, the Order Form, the Configuration Form (if any) and the Tariff (if any).
"Customer"	means the person named on the Order Form. BT may accept instructions from another person who BT reasonably believes is acting with the Customer's authority or knowledge.
"Email"	means any SMTP message sent or received via the Service;
"Member"	means the Customer and its SPEN partners with whom the Customer creates an encrypted network by utilising the Boundary Encryption Service;
"Minimum Period"	means the first 12 months of the Service beginning on the Operational Service Date or any other minimum period specified in the Service Schedule.
"Normal Working Day"	means Monday to Friday excluding public holidays as recognised in England;
"Normal Working Hours"	means between 08:00 and 17:00 UK time each Normal Working Day;
"Open Relay"	means an Email server configured to receive Email from an unknown or unauthorised third party and forward the Email to one or more recipients that are not users of the Email system to which that Email server is connected. Open Relay may also be referred to as "Spam relay" or "public relay";
"Operational Service Date"	means the date when the Service is first made available to the Customer at a Site, or the date when the Customer first starts to use the Service, whichever is the earlier.
"Order Form"	means the form that details the Service to be ordered by the Customer which when signed by both parties will be part of this Contract.
"Order Form Amendment"	means a form signed by both parties which details any variations to the Conditions, the Order Form, the Configuration Form or the Service Schedule made in accordance with paragraph 18 of this Contract.
"Planned Maintenance"	means periods of maintenance of which the Customer has been given seven (7) days prior notification by BT and which may cause disruption of Service due to non availability of the Designated Tower Cluster. Planned Maintenance shall not accumulate to more than eight (8) hours per calendar month and in any case shall not take place between 8am and 6pm local time;
"Registered Usage"	The number of Users agreed between the Customer and BT as being scanned by the Service.
"Service"	means the service or, where appropriate, part of the service described in the Service Schedule to this Contract.
"Service Schedule"	means the schedule to this Contract which contains the description of the Service to be provided by BT
"Spam"	means unsolicited commercial Email;
"Tower"	means a cluster of load balanced servers, configured to provide the Services;
"User"	means a person or mailbox on behalf of which Email or Web requests are being scanned by the Service; and
"Virus"	means a piece of program code, including a self-replicating element, usually (but not necessarily) disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is designed so that it may infect other computer systems;

1.2 References to Sections, Paragraphs, Sub-Paragraphs, Schedules and Appendices are to the sections, paragraphs, sub-paragraphs of and schedules and appendices to, this Contract.

1.3 Headings are for convenience only and shall be ignored in interpreting this Contract.

1.4 This Contract begins on the date that the Order Form is signed by both parties and will continue until terminated in accordance with this Contract.

2 Supply of Service

2.1 BT will provide the Service to the Customer on the terms of this Contract.

2.2 BT will use reasonable endeavours to provide the Service by the date agreed with the Customer, but all dates are estimates and BT has no liability for any failure to meet any date, unless the Service Schedule provides otherwise.

2.3 BT will provide the Service with the reasonable skill and care of a competent telecommunications service provider.

2.4 BT will use reasonable efforts to provide uninterrupted Service but from time to time faults may occur, which BT will rectify in accordance with the timescales described in schedule 1.

2.5 Occasionally BT may:

(a) for operational reasons, change the codes or the numbers used by BT for the provision of the Service or the technical specification of the Service, provided that any change to the technical specification does not materially affect the performance of the Service;

(b) temporarily suspend the Service because of an emergency or for operational reasons maintenance or improvements. Service will be restored as soon as possible.

Before doing any of these things, BT will give the Customer as much notice as possible.

2.6. BT reserves the right both prior to the provisioning of the Service and at any time during the supply of the Service to test whether the Customer's Email systems allow Open Relay. If at any time the Customer's Email systems are found to allow Open Relay, BT will inform the Customer and reserves the right to withhold provision of or suspend all or part of the Service immediately and until the problem has been resolved.

2.7. If at any time the Customer's Email systems are found to be being used for Bulk Email or Spam, BT will inform the Customer and reserves the right to withhold provision of or suspend all or part of the Service immediately and until such use is terminated. For the avoidance of doubt the sending of Spam or Bulk Email will constitute material breach of this Contract as per Paragraph 12.1a) below.

2.8. If at any time continued provision of the Service would compromise the security of the Service due, without limitation, to hacking attempts, denial of service attacks, mail bombs or other malicious activities either directed at or originating from the Customer's domains the Customer agrees that BT may temporarily suspend Service to the Customer. In such an event, BT will promptly inform the Customer and will work with the Customer to resolve such issues, re-instating Service at the earliest opportunity.

2.9. Subject to applicable legislation, BT may provide the Service from any hardware installation forming part of the Service anywhere in the world and may, at any time, transfer the provision of the Service from one installation to another. BT does not guarantee that any such installation, or part thereof, is dedicated to the sole use of the Customer.

2.10.In order to fulfil its obligations in managing the Service, BT may at any time amend the Service and any documentation relating thereto for any reason including, but not limited to: legal; safety; business; or technical considerations.

2.11.Should the Service be suspended or terminated for any reason whatsoever, BT shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of the Customer to undertake all other necessary configuration changes to their mail servers, and to inform their ISP of the need to reroute internet traffic.

3 Customer's Obligations

3.1. The Customer must comply with all reasonable instructions, which BT believes are necessary for reasons of health, safety or the quality of any telecommunications service provided by BT to the Customer or any other customer.

3.2. In consideration of BT supplying the Service to the Customer, the Customer shall pay BT'S charges from time to time in accordance with Paragraph 5 below.

3.3. The Customer will provide BT with all technical data and all other information BT may reasonably request from time to time to allow BT to supply the Service to the Customer. All information the Customer supplies will be complete, accurate and given in good faith. Such information will be treated as Confidential Information under the terms of this Contract.

3.4. The Customer shall not allow its Email systems to:

a) act as an Open Relay;

b) send or receive Bulk Email instigated by the Customer; or

c) send Spam

Should the Customer fail to meet these obligations and disruption occur to the Service then, in addition to BT rights to suspend the Service in Paragraphs 2.6, 2.7 and 12.1a) below, BT reserves the right to charge the Customer at BT's then current rates for any remedial work which becomes necessary as a direct result of the Customer's failure to meet these obligations.

3.5. The Customer recognises that information sent to and from the Customer will pass through the Service and accordingly the Customer agrees to use the Service for legitimate business purposes and:

a) comply with all relevant legislation applicable to use of the Internet;

b) conform to the protocols and standards published on the Internet from time to time and adopted by the majority of Internet users; and

c) indemnify BT against any liability to third parties resulting from information passing through the Service from the Customer.

3.6. The Customer agrees that the Customer will not use the Service for any unlawful purpose or in breach of the laws of England and Wales or any other law applicable to the use of the Internet. These prohibited uses include, but are not limited to:

a) civil and criminal offences of copyright and trademark infringement;

b) transmission, display or publication of obscene material;

commission of any criminal offence under the Computer Misuse Act 1990 or similar legislation in any country;

c) any transmission, display or publication of any material which is of a defamatory, offensive, abusive or menacing character to any other person;

d) transmission, display or publication of any material in breach of the Data Protection Act 1998 (or any replacing statute) dealing with data protection or similar legislation in any other country or of any material which is confidential or is a trade secret; or

e) use of the Service in any manner which is a violation or infringement of the rights of any individual, organisation or company within the United Kingdom and elsewhere.

3.7. The Customer agrees to indemnify BT against all and any losses, costs and expenses BT may incur as a result of any breach by the Customer of Paragraph 3.6.

3.8. In addition to BT'S termination rights set out in Paragraph 12 below, BT may, at any time and at BT sole option, suspend the Service until the Customer gives suitable undertakings and provides security in terms satisfactory to BT to comply with the Customer's obligations in this Paragraph 3 or terminate the Service if the Customer is in breach of any of the obligations set out herein. On any termination in accordance with this Paragraph 3.8 the provisions of Paragraph 12.2 and 12.3 below will apply in respect of the charges payable for the Service.

4 Security

4.1 The Customer is responsible for the security and proper use of all user IDs and passwords used in connection with the Service (including changing passwords on a regular basis) and must take all necessary steps to ensure that they are kept confidential, secure, used properly and not disclosed to unauthorised people.

4.2 The Customer must immediately inform BT if there is any reason to believe that a user ID or password has or is likely to become known to someone not authorised to use it or is being or is likely to be used in an unauthorised way.

4.3 The Customer must not change or attempt to change a user ID. If a Customer forgets or loses a password or user ID the Customer must contact BT and satisfy such security checks as BT may operate.

4.4 BT reserves the right to suspend user ID and password access to the Service if at any time BT has reason to believe that there is or is likely to be a breach of security or misuse of the Service.

4.5 BT reserves the right at its sole discretion to require the Customer to change any or all of the passwords used by the Customer in connection with the Service

4.6 The Customer must immediately inform BT of any changes to the information the Customer supplied when registering for the Service.

5 Charges and Payment

5.1. The charges to be paid by the Customer to BT for the Service will be as shown) on the Order Form.

5.2. BT will commence charging for the Service from the Operational Service Date.

5.3. Charges for the Service shall relate to the Registered Usage. The charges are applicable to normal use of the Service by Users. "Normal use" means that on average a User is unlikely to send or receive more than 200 emails per day on a regular basis. Where on average the Customer's Users send or receive more than 200 emails a day (calculated across the total number of Users over a period of not less than one month), BT reserves the right to increase the Registered Usage accordingly.

5.4. The Customer shall notify BT if at any time (during or after the Minimum Period) the number of Users being scanned exceeds the Registered Usage and BT will increase the Registered Usage accordingly. Additionally, BT will monitor the Customer's actual usage of the Service and if the actual number of Users being scanned exceeds the Registered Usage, BT will increase the Registered Usage accordingly. Where BT increases the Registered Usage, BT will at its sole option raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in Registered Usage on a pro-rata basis for the remaining part of the current invoicing period.

5.5. BT shall apply one-off charges for Customer requested Service configuration changes (including, but not limited to, changes to the Customer's domain names and IP addresses).

5.6. Changes in Registered Usage may be made in multiples of fifty (50) Users.

5.7. Outside the minimum period, BT may revise the charges on 28 days notice to the Customer.

5.8. The Customer will pay the charges within 28 days of the date of BT's invoice. BT may charge daily interest on late payments at a rate equal to 4% per annum above the base lending rate of HSBC Bank plc.

5.9. Unless otherwise stated in the Order Form or an Order Form Amendment, all charges will be invoiced and paid in Pounds Sterling. Value Added Tax or any other applicable in country sales or use tax, surcharge or like charge in a country where the Service is provided which is payable by the Customer will be added to BT's invoices as appropriate.

5.10.BT may, at any time, require the Customer to pay a deposit or provide a guarantee as security for payment of future bills.

5.11. Where the Customer requests BT to investigate a fault, and BT reasonably believes no fault exists or that the cause of the fault is outside the scope of this Service, and BT so advise the customer beforehand, BT reserves the right to charge the Customer for work carried out by BT unless the fault is subsequently found to be within the scope of the Service.

6 Marketing

6.1 The Customer agrees that BT may use the Customer's company name, logo and testimonial (if such testimonial is provided) in BT's promotional material and communications including, but not limited to, proposals, presentations, website and corporate brochure.

7 Conditions of Sale

7.1 The terms of this Contract shall apply to the provision of the Service. Any terms and conditions stated on the Customer's order shall be null and void unless expressly agreed to in writing by BT on its order acknowledgement.

8 Limitation Of Liability

8.1 BT accepts unlimited liability for death or personal injury resulting from its negligence. Paragraphs 8.2 and 8.3 do not apply to such liability.

8.2 BT is not liable to the Customer, either in contract, tort (including negligence) or otherwise for any direct or indirect loss of profits, business or anticipated savings, nor for any indirect loss or damage or for any destruction of data.

8.3 BT's liability to the Customer in contract, tort (including negligence) or otherwise in relation to this Contract is limited to £1 million for any one incident or series of related incidents and to £2 million for all incidents in any period of 12 months

8.4 Each provision of this Contract, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts will continue to apply.

9 Intellectual Property Rights

9.1 The intellectual property rights in the Service and any hardware or software used in connection with the Service is and will at all times remain BT property or that of BT's licensors.

9.2 Where software is provided to enable the Customer to use the Service, BT grants the Customer a non-exclusive, non-transferable licence to use the software for that purpose.

9.3 The Customer will not, without BT's prior written consent, copy, decompile or modify the software, nor copy the manuals or documentation (except as permitted by law).

9.4 The Customer will sign any agreement reasonably required by the owner of the copyright in the software to protect the owner's interest in that software.

10 Intellectual Property Rights Indemnity

10.1 BT will indemnify the Customer against any claims and proceedings arising from infringement of any intellectual property rights through BT's provision of the Service to the Customer. As a condition of this indemnity the Customer must:

a) notify BT promptly in writing of any allegation of infringement;

b) make no admission relating to the infringement;

c) allow BT to conduct all negotiations and proceedings in respect of such claims and give BT all reasonable assistance in doing so (BT will pay the Customer's reasonable expenses for such assistance); and

d) allow BT to modify or replace the Service or any item provided as part of the Service, so as to avoid the infringement, provided that the modification or replacement does not materially affect the performance of the Service.

10.2 If BT does not effect a modification or replacement under paragraph 10.1(d) or procure the right for Customer to continue using the Service, in each case within 90 days of the date it received notice of the infringement, then either party shall be entitled to terminate the Contract by giving 5 days written notice to the other.

10.3 The indemnity in paragraph 10.1 does not apply to infringements caused by the use of the Service in conjunction with other equipment, software or services not supplied by BT or to infringements caused by designs or specifications made by, or on behalf of, the Customer. The Customer will indemnify BT against all claims, proceedings and expenses arising from such infringements.

10.4 The limitations and exclusions of liability contained in paragraph 8 do not apply to this paragraph.

11 Termination of this contract

11.1 Unless otherwise specified in the Service Schedule, either party may terminate this Contract or the Service provided under it on 3 months written notice to the other.

11.2 If the Customer terminates this Contract or the Service at any time prior to the expiry of its Minimum Period (other than due to termination of this Contract under paragraph 11.3 or 11.4 or 11.5) or if BT terminates for the Customer's breach under section 12 before the relevant Minimum Period has expired, the Customer agrees to pay eighty (80) per cent of the monthly rental charges for each of the months remaining in the Minimum Period.

11.3 If the Customer exercises its right of termination under paragraph 11.1 within 14 days of receipt of notice of:

a) BT materially changing the Conditions to the detriment of the Customer under paragraphs 2.5, or 18.2; or

b) BT increasing the total charges payable by the Customer for the Service during the Minimum Period by an amount exceeding 10% per year

then the Customer will not be liable to pay the increase in charges for such 14 day period or for the notice period in paragraph 11.1 and, further, will not be liable for the termination charges specified in paragraph 11.2.

11.4 The customer may terrminate this contract within thirty (30) days from the Operational Service Date. In the case of termination under this Sub-Paragraph 11.4, any amount already paid by the Customer,will be refunded by BT, and the customer will not be liable for the termination charges specified in paragraph 11.2.

11.5 If the Customer exercises its right of termination under paragraphs 10.2 or 14.3 then the Customer will not be liable for the termination charges specified in paragraph 11.2.

11.6 Termination of this Contract shall be without prejudice to any rights or liabilities accrued at the date of termination.

11.7 Upon termination:

a) BT shall be entitled to cancel the provision of Service to the Customer; and

b) all invoices become due and payable;

12 Breaches of this contract

12.1 Either party may terminate this Contract or the Service (or both)

a) immediately on notice, if the other commits a material breach of this Contract, which is capable of remedy, and fails to remedy the breach within a reasonable time of a written notice to do so; or

b) immediately on notice if the other commits a material breach of this Contract which cannot be remedied; or

c) on reasonable notice if the other party is repeatedly in breach of this Contract and fails to remedy the breach within a reasonable time of a written notice to do so; or

d) immediately on notice if the other is the subject of a bankruptcy order, or becomes insolvent, or makes any arrangement or composition with or assignment for the benefit of their creditors, or goes into voluntary (otherwise than for reconstruction or amalgamation) or compulsory liquidation, or a receiver or administrator is appointed over their assets, or if there is a change of control of the Customer, or if the equivalent of any such events under the laws of any of the relevant jurisdictions occurs to the other party.

12.2 If BT is entitled to terminate this Contract under paragraph 12.1, BT may, on giving prior notice where practicable, suspend the Service without prejudice to such rights. Where the Service is suspended under this paragraph the Customer must pay the charges for the Service until this Contract is terminated.

12.3 If this Contract or the Service is terminated by BT at any time prior to the expiry of the Minimum Period because of an event specified in paragraph 12.1 the Customer must pay BT, without prejudice to other rights BT may have, the termination charges specified in paragraph 11.2.

12.4 If either party delays in acting upon a breach of this Contract that delay will not be regarded as a waiver of that breach. If either party waives a breach of this Contract that waiver is limited to that particular breach.

13 Confidentiality

13.1 The parties will keep in confidence any information (whether written or oral) of a confidential nature (including software and manuals) obtained under this Contract and will not, without the written consent of the other party, disclose that information to any person (other than their employees or professional advisers, or in the case of BT, the employees of a BT Group Company, a BT Associate or BT's suppliers who need to know the information).

13.2 This paragraph 13 will not apply to:

a) any information which has been published other than through a breach of this Contract;

b) information lawfully in the possession of the recipient before the disclosure under this Contract took place;

c) information obtained from a third party who is free to disclose it; and

d) information which a party is requested to disclose and, if it did not, could be required to do so by law.

13.3 This paragraph 13 will remain in effect for 2 years after the termination of this Contract.

13.4 BT recognise and confirm that the content of all Emails sent to or received from the Customer by the Service is confidential. In the normal provision of the Service BT would not access, read or copy Emails or their attachments other than by electronic methods for the purposes of providing the Service. However, BT reserve the right to utilise the Virus-related content of such Email or its attachments solely for the purposes of:

a) maintaining and improving the performance and the integrity of the Service;

b) complying with all regulatory, legislative or contractual requirements; and

c) making available to licensors of the Service any information passing through the Service which may be of interest to the licensors solely for the purpose of further developing and enhancing the Service.

13.5 Where BT exercise the foregoing rights BT will use all reasonable endeavours to keep confidential all information received from the Customer or for the Customer in connection with the Service.

14 Matters beyond the reasonable control of either party

14.1 If either party is unable to perform any obligation under this Contract because of a matter beyond that party's reasonable control such as lightning, flood, exceptionally severe weather, fire, explosion, war, civil disorder, industrial disputes or acts of local or central Government or other competent authorities, or events beyond the reasonable control of that party's suppliers, that party will have no liability to the other for that failure to perform.

14.2 In the event of:

(a) a refusal or delay by a third party to supply a telecommunications service to BT and where there is no alternative service available at a reasonable cost; or

(b) the imposition of restrictions of a legal or regulatory nature which prevent BT from supplying the Service

then BT will have no liability to the Customer for failure to supply the Service.

14.3 If any of the events detailed in paragraphs 14.1 or 14.2 continue for more than 3 months either party may serve notice on the other terminating this Contract.

15 Dispute Resolution

15.1 If a dispute arises between the parties to this Contract, the parties will use their reasonable endeavours to settle the dispute in accordance with the following procedures:

a) a dispute which has not been settled by the Customer's representative and the BT representative within 7 days of the matter being raised, may be escalated by either party to the first level by written notice to the other party;

b) if the dispute is not resolved at the first level within 7 days of escalation either party may refer the dispute to the second level.

The parties' representatives and the people to whom a dispute must be escalated at the first and second levels will be as notified to each other in writing, from time to time.

15.2 If a dispute is not resolved after the procedures set out in paragraph 15.1 have been followed then, if the parties agree, the dispute will be referred to a mediator:

a) the mediator will be appointed by agreement of the parties. In the event of a failure to agree within 3 days of a proposal by one party, the mediator will be appointed by the Centre for Dispute Resolution (CEDR);

b) within 14 days of the appointment of the mediator the parties will meet with the mediator in order to agree the procedure to be adopted for the negotiations;

c) all negotiations connected with the dispute will be conducted in confidence and without prejudice to the rights of the parties in any further proceedings;

d) if the parties reach agreement on the resolution of the dispute the agreement will be put in writing and once signed by the parties will be binding on them;

e) if the parties are not prepared to agree to the dispute being referred to a mediator, or fail to reach agreement within 2 months of the mediator being appointed then either party may exercise any remedy that it has under this Contract.

16 Data Privacy and Regulation of Investigatory Powers

16.1 The Customer shall take all necessary measures to ensure that it, and all its employees, are aware of any responsibilities they have in respect of data protection and privacy laws and/or regulations and as BT has no control or influence over the content of the Emails processed by the Service the Customer shall hold BT harmless for any claims by any party relating thereto.

16.2 As required by law, the Customer shall use all reasonable efforts to ensure it informs (for example via a banner message on Emails) those who use any communications system covered by the Service, that communications transmitted through such system maybe intercepted, and indicate the purposes of such interception. The Customer shall hold BT harmless from any claims from its employees, any third party and/or governmental agencies relating to such interceptions. The Customer shall not use, or require BT to use, any data obtained via the Service for any unlawful purposes.

17 Export Control

17.1 Provision of the Service to the Customer may be subject to export control law and regulations. BT does not represent that any necessary approvals and licences will be granted. The Customer will provide reasonable assistance to BT to obtain any necessary consents. If, through no fault of BT, any necessary consents are not granted, then BT can terminate this Contract or the provision of the Service under it (as appropriate) without any liability to the Customer.

17.2 The Customer agrees not to disclose or re-export to any country, directly or indirectly any BT Equipment or item provided with or as part of the Service, without complying with the export rules of the government of the country from which the disclosure or re-export is made.

18 Changes to this contract

18.1 (a) Except in the circumstances described in paragraphs 2.5 (a), 5.2 and 18.2 if either party wishes to vary this Contract including the specification of the Service it must notify the other party in writing, detailing the proposed change and the reason for it.

(b) The parties will discuss the proposed change.

(c) Within a reasonable time of receipt of a proposed change, or the date of the discussions under paragraph 18.1(b), the receiving party will notify the other party in writing whether the proposed change is feasible and the likely financial, contractual, technical or other effects of the proposed change.

(d) Within a reasonable time of notification of the effects of a proposed change the receiving party will advise the other party whether it wishes this Contract to be amended to incorporate the change.

(e) Where the parties agree a change to this Contract it will be recorded on an Order Form Amendment and will form part of this Contract when signed by both parties.

18.2 Where this Contract is entered into in a country where BT is obliged by law or by its agreement with a public telecommunications operator to trade with all its customers for the Service on the same or particular terms then BT may amend this Contract on 28 days notice to the Customer and paragraph 18.1 will not apply.

19 Transfer of Rights and Obligations

19.1 Neither party may transfer its rights or obligations under this Contract, without the written consent of the other, except that BT may transfer its rights or obligations (or both) to a BT Group Company without the Customer's consent.

20 Waiver

20.1 The failure of a party to exercise or enforce any right under this Contract shall not be deemed to be a waiver of that right nor operate to bar the exercise or enforcement of it at any time or times thereafter.

21 Entire Agreement

21.1 This Contract contains the whole agreement between the parties and supersedes all previous written or oral agreements relating to its subject matter.

21.2 The parties acknowledge and agree that:

(a) they have not been induced to enter into this Contract by any representation, warranty or other assurance not expressly incorporated into it; and

in connection with this Contract their only rights and remedies in relation to any representation, warranty or other assurance are for breach of this Contract and that all other rights and remedies are excluded.

21.3 The provisions of paragraphs 21.1 and 21.2 shall not affect the parties rights or remedies in relation to any fraud or fraudulent misrepresentation

21.4 A person who is not a party to this Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Contract but this does not affect any right or remedy of a third party which exists or is available apart from that Act.

22 Severability

22.1 If any provision of the Contract shall be held to be invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed from the Contract and the remaining provisions shall continue in full force and effect as if this Contract had been executed with the invalid, illegal or unenforceable provisions omitted and the parties shall promptly negotiate a replacement.

23 Notices

23.1 Notices given under this Contract must be in writing and may be delivered by hand or by courier, or sent by first class post to the following addresses:

(a) to BT at the address of the BT office shown on the Order Form or any alternative address which BT notifies to the Customer;

(b) to the Customer at the address to which the Customer asks BT to send invoices, the address of the Site or, if the Customer is a limited company, its registered office.

23.2 A notice shall be duly served:

if delivered by hand or by courier, at the time of delivery; and

if sent by first class post, three working days after the date of posting.

24 Governing Law and Jurisdiction

24.1 This Contract shall be governed by and construed in accordance with the laws of England and Wales and each party submits to the exclusive jurisdiction of the English Courts.

Schedule 1
Service Schedule - General

1. Introduction

BT is a Telecommunications and Managed Services Provider which includes services offering internet-level Email and Web security.

The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis. The Service is monitored for hardware availability, service capacity and network resource utilisation. Regular adjustments are made to the Service to ensure its optimum efficiency is maintained.

The Service is available to Customers who are permanently connected to the Internet with a fixed IP address. It cannot be provided to Customers who's Email systems are connected to the Internet via dial-up or ISDN lines or whose IP address is dynamically allocated.

2 Management

For all incoming Email the IP reputation of the sender is ascertained. Email originating from a disreputable source (such as a spammer) will be slowed down to minimise network capacity impact. The Customer's inbound Email may be scanned using a number of different detection methods to determine whether or not it is Spam. If an inbound Email is suspected as being Spam, one of a number of actions will be taken depending on the configuration options selected by the Customer. The configuration options are listed in Paragraph 3.2 of Appendix 3 below and are accessible by the Customer through ClientNet.

Wherever possible, Planned Maintenance will be carried out without affecting the Service. This will generally be achieved by carrying out Planned Maintenance during periods of anticipated low traffic and by carrying out Planned Maintenance on part, not all, of the network at any one time. During Planned Maintenance periods the traffic may be diverted round sections of the network not undergoing maintenance in order to minimise disruption to the Service.

Where emergency maintenance is necessary and is likely to affect the Service, BT will endeavour to inform the affected parties and will post an alert message on ClientNet as soon as possible and in any case within one (1) hour of the start of the emergency maintenance.

3 ClientNet

An integral part of the Service is the internet-based configuration, management and reporting tool called ClientNet. ClientNet is made available to the Customer via a secure password protected login which should not be disclosed to a third party. ClientNet provides the facility for the Customer to view data and statistics on their use of the Service and offers a number of configuration and management facilities.

4 Fault reporting

BT will on a twenty-four (24) hours/day by seven (7) days/week basis:

a) receive reports from the customer relating to problems with the Service; and
b) liaise with the Customer to resolve such problems.

BT will endeavour to answer 85% of calls within thirty-five (35) seconds and the remaining 15% of calls within sixty (60) seconds.

BT will use reasonable endeavours to respond to problems and enquiries in accordance with the following timescales:

Priority Level	Definition	Response Target
Critical	Loss of Service that cannot be circumvented	Responded to within 2 hours
Major	Loss of Service that can be circumvented, partial loss of Service or Service impairment	Responded to within 4 hours
Minor	Potentially Service affecting	Responded to within 1 working day
Information	Non-Service affecting information request	Responded to within 2 working days

5 Customer Service

BT will provide customer service during Normal Working Hours to:

a) receive and process orders for provisioning the Service;
b) receive and process requests for modifications to the operational aspects of the Service; and
c) respond to billing and invoicing queries.

Unless stated otherwise in the relevant Service Description, on receipt of a fully completed and actionable order or Service Change Request, the BT Customer Service team will aim to provision the Service within three (3) Normal Working Days, providing all the phases of technical due diligence have been completed.

Schedule 2
Service Schedules (Service Specific)

Appendix 1
Email Anti-Virus Service

1. Overview

The Email Anti-Virus service ("Email AV") is BT's internet-level Email Virus scanning service. The Customer's inbound and outbound Email including all attachments, macros or executables are directed through the Email AV service using DNS and MX record settings.

Email and attachments are electronically routed via the BT Managed Email Security scanning Towers and digitally examined. The Email and attachments are scanned by multiple industry leading anti-virus products and proprietary technology.

2 Alert Messages

If a Customer's inbound Email or attachments are found to contain a Virus, an automatic alert may, if selected by the Customer, be despatched to the sender and intended recipient by way of notification. With a Customer's outbound Email the Service may notify the sender only and not the intended recipient. User notifications may also be sent to an Email administrator in both cases. The infected Email is forwarded to a secure server pending automatic destruction after seven (7) days, provided that it is not transported as a mass mailer virus, in which case it will be deleted immediately.

In the case of a major breakout of a new Virus, an alert message will be posted on ClientNet.

3 Configuration

ClientNet can be used for customising banner texts, releasing Virus-infected Email and setting maximum Email sizes.

4 Releasing a Virus-Infected Email

Where a Virus-infected Email is shown to be releasable, it can be released from the secure server using ClientNet. The Email will be released either to the first address of the original recipient list or to a specified address previously notified to BT and logged by BT in ClientNet (Note: these addresses may be group Email names or aliases in which case the Email will be released to all addressees in the group or alias). Optionally the Virus-infected Email may be released to an alternative address by BT on receipt of the appropriate Release Authorisation Form. BT will only act on requests authorised by Customers to forward Virus-infected Email. BT will not return Virus-infected Email to the sender. BT will not forward Virus-infected Email to third parties. Certain Virus-infected Emails sent to the customer are not releasable due to them containing a Virus which is particularly infectious or damaging. These are shown on ClientNet as being not releasable.

5 Email AV Terms and Conditions

The Customer agrees to indemnify BT against all and any losses, costs and expenses BT may incur as a result of the intentional release of a Virus-infected Email under Paragraph 0 above.

If requested to release a Virus-infected Email, BT will release it within eight (8) Normal Working Hours of receipt of a duly authorised release request.

Appendix 2
Email Image Control Service

1. Overview

The Email Image Control service ("Email IC") is BT'S internet-level Email anti-porn service which is designed to detect pornographic images contained in image files.

2 Service Description

The Customer's inbound and outbound Email can be scanned using Image Composition Analysis (ICA) for pornographic images contained in image files attached to Email.

If a Customer's inbound or outbound Email is suspected to contain a pornographic image, one of a number of actions will be taken depending on the configuration options selected by the Customer.

3 Configuration

On receipt of a fully completed and accepted order, BT will enable Email IC for the Customer. Initially Email IC will be enabled for each of the Customer's domains. The Customer is responsible for setting the configuration options for Email IC for each domain according to the Customer's needs. The Customer configures Email IC using ClientNet.

Options are available for specifying the level of detection sensitivity. Sensitivity can be set to High, Medium or Low. These settings are particularly subjective, however, as a guide more images will be suspected to be pornographic at High sensitivity and fewer images will be suspected to be pornographic at Low sensitivity.

Options are available for defining the actions to be taken on detecting a suspected pornographic image. These options may be set independently for inbound and outbound Email and should be set in line with the Customer's existing Acceptable Computer Use Policy (or its equivalent). These options are:

a) log suspected Email (provides statistics viewable via ClientNet)

b) tag suspected Email within the header (for inbound Email only)

c) copy suspected Email to a pre-defined Email address

d) redirect suspected Email to a pre-defined Email address

e) delete suspected Email.

4 Reporting

If the chosen options in Paragraph 3 of this Appendix are to redirect or delete Email containing a suspected pornographic image, then an automatic alert will be despatched to the sender. If the Email is inbound to the Customer an automatic alert is also sent to the intended recipient.

Reporting on the effectiveness of Email IC is provided through ClientNet where statistics are available on the numbers of inbound and outbound Emails suspected of containing pornographic images. ClientNet may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

5 Email IC Terms and Conditions

NO PORNOGRAPHIC IMAGE DETECTION SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT A PORNOGRAPHIC IMAGE OR FOR WRONGLY IDENTIFYING AN IMAGE AS SUSPECTED TO BE PORNOGRAPHIC WHICH PROVES SUBSEQUENTLY NOT TO BE SO. Furthermore the Customer agrees to indemnify BT for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any suspected pornographic or non-pornographic image except where such claim arises due to BT breach of contract or negligent act or omission.

It may not be possible to scan attachments with content which is under the direct control of the sender (for example, password protected and/or encrypted attachments).

Email IC is not able to scan for pornographic images embedded in other documents.

BT emphasises that the configuration of Email IC is entirely in the control of the Customer. Email IC is intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so BT advises the Customer to always check their local legislation prior to deploying Email IC. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Email IC. The Customer recognises that the definition of what does and what does not constitute a pornographic image is subjective. The Customer should take this into consideration when configuring the Service.

If the Customer releases or requests the release of a Virus-infected Email, the released Email will not be scanned by Email IC prior to release.

Appendix 3
Email Anti Spam Service

1. Overview

The Email Anti-Spam service ("Email AS") is BT's internet-level Email Anti-Spam service which is designed to protect the Customer from unsolicited or unwanted Email.

2 Service Description

A private approved senders list may be compiled by the Customer. If this detection method is selected and an incoming Email is received from an approved senders listed domain, it will automatically bypass any other selected Spam detection methods.

A private blocked senders list may be compiled by the Customer. If this detection method is selected and an incoming Email is received from a blocked sender listed domain an action will be taken as defined by the configuration options in Paragraph 0 below.

A number of public blocked senders lists may be used. If any of these detection methods are selected and an incoming Email is received from a domain listed on one of the selected public blacklists an action will be taken as defined by the configuration option in Paragraph 0 below.

If the Email has not been deleted as a result of being blocked as above and the signaturing system is selected and the action that would be taken as a result of detecting the Email as Spam is more severe than that already selected as a result of blocked senders list detection, the Customer's inbound Email is scanned using the signaturing system. If an Email is detected by this method as being Spam then action will be taken as defined by the configuration options in Paragraph 0 below. This action will supersede any less severe action previously allocated by any of the blocked senders list methods.

If the Email has not been deleted as a result of the preceding processes and heuristics detection is selected and the action that would be taken as a result of detecting the Email as Spam as configured by the Customer is more severe than that already selected as a result of detection by the preceding processes, the Customer's inbound Email is scanned using heuristics scanning. If an incoming Email is heuristically detected as being Spam action will be taken as defined by the configuration options in Paragraph 0 below. This action will supersede any less severe action previously allocated by any of the preceding methods.

Blocked senders/approved senders lists provided by BT are given as examples only.

3 Configuration

On receipt of a fully completed and accepted order, BT will enable Email AS for the Customer. Initially Email AS will be enabled for each of the Customer's domains. The Customer is responsible for setting the configuration options for Email AS for each domain according to the Customer's needs. The Customer configures Email AS using ClientNet.

Options are available for specifying the actions to be taken should an Email be suspected as being Spam. These options, listed below, are selectable for each of the available detection methods:

a) tag suspected Email within the header

b) tag suspected Email within the subject line;

c) redirect suspected Email to a pre-defined Email address (which must be on a domain being scanned by the Service);

d) delete suspected Email;

e) Spam Quarantine.

4 Spam Quarantine Service Description

If the Customer configures Spam Quarantine for a domain, each User's Spam Quarantine account will be set up automatically upon the first time that suspected Spam is identified by the Email AS service and the User will automatically receive an Email notification.

Spam Quarantine is accessed by the User via the Spam Manager interface.

Suspected Spam can be stored for a maximum of fourteen (14) days after which it will be automatically deleted.

If Spam Quarantine is not able to accept Email the suspected Spam will be tagged and sent to the recipient.

5 Spam Quarantine Configuration

The Customer configures Spam Quarantine via ClientNet.

The User may at any time select one of the following notification options:

a) Notifications to be received daily;

b) Notifications to be received at various frequencies;

c) Notifications not to be received.

The following release options are available through Spam Manager:

a) Delete Email;

b) Release Email to original recipient address;

c) Review text of Email.

In order to utilise Spam Quarantine the Customer must have registered an Address Validation list with BT. The Address Validation list comprises all valid Email addresses utilised by the Customer. Any recipient address not on the list is deemed invalid and Email will not be delivered to that address.

Through ClientNet a Customer may control other aspects of Spam Manager:

a) Automated or manual notification policy;

b) Setup of summary notifications;

c) Default language settings;

d) Approved senders list requests;

e) preset alias emails and

f) specialised Users (eg Quarantine Administrators).

6 Reporting

Reporting on the effectiveness of Email AS is provided through ClientNet. ClientNet may be configured to generate reports which are sent by Email to the Customer on a weekly or monthly basis.

7 Email AS Terms and Conditions

NO ANTI-SPAM SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT SPAM OR FOR WRONGLY

IDENTIFYING AN EMAIL SUSPECTED AS BEING SPAM WHICH PROVES SUBSEQUENTLY NOT TO BE SO. Furthermore the Customer agrees to indemnify BT for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any item suspected as being Spam except where such claim arises due to BT breach of contract or negligent act or omission.

BT emphasises that the configuration of Email AS is entirely in the control of the Customer. BT recommends that the Customer has an Acceptable Computer Use Policy (or its equivalent) in place. In certain Countries it may be necessary to obtain the consent of individual personnel and so BT advises the Customer to always check their local legislation prior to deploying Email AS. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Email AS.

Appendix 4
Email Content Control Service

1. Overview

Email Content Control ("Email CC") is BT's content control service designed to enable the Customer to configure their own rule based filtering strategy in line with their Acceptable Use Policy (or its equivalent) in relation to Email.

2 Service Description

Content Control allows a Customer to build a collection of rules upon which incoming and outgoing Email is filtered in accordance with the service description contained in this Schedule 1. A rule is an instruction set up by the Customer which is used to identify a particular format of message/attachment or content which has prescribed to it a particular course of action to be taken in relation to the Email.

3 Configuration

On receipt of a signed Amendment BT will enable Content Control for each of the Customer's applicable domains. The Customer is responsible for implementing the configuration options for Content Control for each domain according to the Customer's needs. The Customer configures Content Control via ClientNet.

The Customer may configure rules on a 'per domain', 'per group' or 'individual' basis.

Changes made by the Customer to the rules will become effective within 24 hours of such change being made.

Options are available for defining the action to be taken upon detecting a suspected Email. These options may be set independently for inbound and outbound Email and should be set in line with the Customer's existing Acceptable Use Policy (or its equivalent). These options are:

a) Block and delete suspected Email;

b) Tag (if inbound) and redirect suspected Email to administrator;

c) Tag (if inbound) and copy suspected Email to administrator;

d) Tag (if inbound) header of suspected Email;

e) Compress Email attachments;

f) Log only to ClientNet statistics.

g) Tag in the subject line

4 Reporting

Through ClientNet a Customer will be able to review the results of their rules in the form of daily, weekly, monthly and annual summaries organised by both rule and by User.

Reports containing service activity logs can be generated on a weekly or monthly basis and emailed to the Customer upon request.

5 Content Control Support

This Service includes:

a) Walk through of the Content Control interface including a Service description and Q&A session;

b) Normal Working Hours support of core Service. **Note:** this does not include any analysis of the effectiveness of rules.

User Guide.

6 Content Control Terms and Conditions

Suggested word lists and template rules supplied by BT contain words which may be considered offensive. The Customer agrees to indemnify BT against any damages (including reasonable costs) that may be awarded to any third party (including any employee of the Customer) in respect of any claim or action arising out of supply to the Customer of such word lists or rules.

Customer accepts and agrees that BT may compile and publish default word lists using words obtained from the Customers' custom word lists.

The Customer recognises that if Content Control is used in conjunction with the quarantine action of the Anti-Spam service, this may result in suspected Spam being quarantined before it has been filtered by the Content Control service.

BT EMPHASISES THAT THE CONFIGURATION OF CONTENT CONTROL IS ENTIRELY UNDER THE CONTROL OF THE CUSTOMER AND THAT THE ACCURACY OF SUCH CONFIGURATION WILL DETERMINE THE ACCURACY OF THE CONTENT CONTROL SERVICE, THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF THE SERVICE TO DETECT OR WRONGLY IDENTIFY AN EMAIL CONTAINING SUSPECTED CONTENT WHICH PROVES SUBSEQUENTLY NOT TO BE SO. Furthermore the Customer agrees to indemnify BT for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any Email scanned by Content Control.

BT recommends that the Customer has an Acceptable Computer Use Policy (or its equivalent) in place governing its Users' use of Email and that any template rules supplied by BT support such policy. In certain countries it may be necessary to obtain the consent of individual personnel and so BT advises the Customer to always check their local legislation prior to deploying Content Control. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of Content Control.

Appendix 5

Volume Mail Service

1 Overview

The Volume Mail Service is designed to scan Customer's inbound and outbound volume mail

2 Volume Mail Terms And Conditions

A Customer's Volume Mail must be made up of confirmed, opt-in solicited recipients only. The Customer shall, upon BT's request and subject to applicable legislation, provide evidence of such confirmations. This confirmation should be provided within a reasonable period of time from the date of BT's request;

The size of each Volume Mail including attachments must not exceed 500 kilobytes;

The 'Recipients' box on each single Volume Mail must not contain over five hundred (500) Email addresses;

The Customer must operate an effective list management system including the prompt removal of invalid and subscription cancellation email addresses;

The Customer must receive the Email Anti Virus Service for its standard Email;

The Customer's Volume Mail must originate from or be directed towards a separate domain to their standard Email enabling the Volume Mail to be pointed towards a specially provisioned Control Tower;

The default outbound banner shall notify the recipient that the Volume Mail has been virus scanned.

If the Customer subscribes to bands that allow greater than 250,000 reciepients per month, the Customer must send or receive Volume Mail in batches of no more than 250,000 recipients per day;

The Customer recognises and accepts that the sending of Volume Mail is likely to have a varying effect on the flow of Email traffic. Such effects are outside of the control of BT and for this reason BT cannot guarantee service levels;

If at any time (i) the Customer's Email systems are blacklisted, or (ii) the Customer causes the BT systems to become blacklisted due to the sending of Spam, or (iii) the Customer fails to meet any of the obligations set out in this Clause, BT reserves the right at its sole discretion to withhold provision of, suspend or terminate all or part of the Service to the affected Customer immediately.

Appendix 6
Web Anti Virus and Anti Spyware Service

1. Overview

Once the relevant configuration changes are made requests for Web pages and attachments are electronically routed via the Web Anti Virus and AntiSpyware Service ("WebAVAS") and digitally examined for viruses and spyware.

2 Service Description

The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Service. Other content routed though HTTP (for example streaming media) can also be passed through the Service but shall not be scanned.

WebAVAS will scan the first 50Mb of each file transfer. Where files are downloaded that exceed 50Mb in size, the initial 50Mb will be scanned and the remainder passed through if no infections are found in the initial 50Mb.

Outbound communications passing through the proxy shall be examined to determine if it represents Spyware communication. Where this is identified it shall be blocked.

3 Configuration

The configuration settings required to direct this external traffic via the Service are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Service. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to their own infrastructure to facilitate this.

Access to the Service is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings. Where the IP address of the originating user is concealed via Network Address Translation, Proxy Server or otherwise, this service will not be able to distinguish between individual users for the purposes of applying policies or providing reports.

WebAVAS will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages, content or attachments (for example, password protected). Attachments specifically identified as unscannable will be blocked. Streamed and encrypted traffic (i.e. Streaming Media and/or HTTPS/SSL) cannot be scanned and will be passed through WebAVAS unscanned.

4 Alerts

If a Customer's Web page or attachments are found to contain a Virus or Spyware (or deemed unscannable, bar SSL traffic), then access to that Web page or attachment is denied and the Internet user will be displayed an automatic alert Web page in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page, but access to the infected page or attachment will still be denied.

5 General Terms and Conditions

NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF WebAVAS TO DETECT VIRUSES OR SPYWARE OR FOR WRONGLY IDENTIFYING VIRUSES OR SPYWARE. Furthermore the Customer agrees to indemnify BT for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any web page suspected as containing a virus except where such claim arises due to BT breach of contract or negligent act or omission.

BT emphasises that the configuration of WebAVAS is entirely in the control of the Customer. The services described in this Appendix are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so BT advises the Customer to always check their local legislation prior to deploying WebAVAS. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of WebAVAS.

Appendix 7
Web URL Filtering Service

1. Overview

Once the relevant configuration changes are made requests for Web pages and attachments are electronically routed via the Web URL Filtering Service ("WebURLv2") and digitally examined.

2 Service Description

The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through WebURLv2.

3 Configuration

The configuration settings required to direct this external traffic via WebURLv2. are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed via the Service. Where the Customer has Internet services that mandate a direct connection rather than via a proxy, it is the responsibility of the Customer to make the necessary changes to their own infrastructure to facilitate this.

Access to WebURLv2. is restricted via Scanning IP i.e. the IP address(es) from which the Customer's web traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings. Where the IP address of the originating user is concealed via Network Address Translation, Proxy Server or otherwise, this service will not be able to distinguish between individual users or groups for the purposes of applying policies or providing reports.

The Customer is able to configure WebURLv2 to create access restriction policies (based both on categories and types of content) and deploy these at specific times.

4 Alerts

If a User requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the User will be displayed an automatic alert Web page in accordance with the specification below. In rare cases, and where one or more elements of the requested content is blocked, it may not be possible to display the alert Web page, but access to the relevant page will still be denied.

5 General Terms and Conditions

NO WEB SCANNING SOFTWARE CAN GUARANTEE A 100% DETECTION RATE AND THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY DAMAGE OR LOSS RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF WebURL TO DETECT BLOCKED URLs OR CONTENT. Furthermore the Customer agrees to indemnify BT for any damages (including reasonable costs) that may be awarded to any third party in respect of any claim or action arising out of delivery or non-delivery of any web page suspected as constituting a blocked URL or containing blocked content except where such claim arises due to BT breach of contract or negligent act or omission.

BT emphasises that the configuration of WebURL is entirely in the control of the Customer. The services described in this Appendix are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). In certain Countries it may be necessary to obtain the consent of individual personnel and so BT advises the Customer to always check their local legislation prior to deploying WebURL. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of WebURL.

Appendix 8

Policy Based Encryption Service

1 Overview

BT's Policy Based Encryption Service ("PBE") provides the ability to send and receive encrypted Emails based on the Customer's email security policy.

In order to receive PBE, the Customer must also subscribe to the Boundary Encryption ("BE") and Email Content Control ("Email CC") services.

PBE provides the following functionality:

a) Ability to use Email CC to define outbound encryption policies for Emails;

b) Encrypted Email delivery through to the external recipient's inbox;

c) Recipient gains access to the encrypted Email via a secure web portal;

d) Recipient can access the secure web portal to respond to the Email in an encrypted format.

2 Service Description

PBE allows the Customer to send an encrypted Email directly into a recipient's inbox without the need for the recipient to download software.

The Customer can configure the encryption method to be either Push or Pull. For PBE Z, the Email CC rule decides between Push or Pull. For PBE E, the default encryption method is Push but can be changed to Pull by the recipient by downloading the Secure Reader functionality within the recipient's secure web portal.

The "PBE Push" variant of the PBE Service sends the recipient an email notification with the original Email saved within it as an encrypted attachment. Following initial registration online, the recipient is able to view the decrypted Email offline using a Java application on their desktop.

The "PBE Pull" variant of the Service sends the recipient an email notification. The recipient is able to view the decrypted Email online via a secure SSL session in their browser when they log on to a secure web portal and enter their password.

PBE also enables a recipient to enter a secure web portal and respond to an encrypted Email in an encrypted format.

The Customer may brand the portal that recipients use to read their encrypted Emails (for example to include the Customer's logo and support numbers).

The recipient of an encrypted Email may also send a brand new Email to any of the Customer's PBE Users.

If the Customer subscribes to PBE E, a third party Outlook Plug-In is available which adds an "encrypt" icon to the recipient's Outlook toolbar. The Customer acknowledges and agrees that BT is not responsible for such third party software.

If the Customer subscribes to PBE E, a recipient can choose the language of the recipient's secure web portal and notification emails from a list of supported languages.

3 Provisioning and Change Requests

The lead time for provisioning PBE orders and PBE change requests shall be four (4) weeks from the date of BT's acceptance of each order/ change request, provided that all technical due diligence has been completed by the Customer.

The Customer agrees to provide all necessary resources, information, and authorizations, as required, and to activate or correct its DNS mail services for connectivity to PBE.

The Customer may change the branding of the portal a maximum of twice per annum.

4 Configuration

The Customer is responsible for implementing the configuration of PBE according to the Customer's needs. The Customer configures PBE via ClientNet by selecting the options available under the Email CC Service.

BT emphasises that the configuration of PBE is entirely under the control of the Customer and that the accuracy of such configuration will determine the accuracy of PBE. The Customer acknowledges and agrees that BT can therefore accept no liability for any damage or loss resulting directly or indirectly from any failure of PBE to fulfil the Customer's encryption obligations.

5 Service Parameters

The following limitations apply to PBE:

a) The number of secure Emails the Customer may send in any month using PBE Z may not exceed three hundred (300) times the number of Users purchased for PBE. The number of secure Emails the Customer may send in any month using PBE E may not exceed two hundred and forty (240) times the number of Users purchased for PBE. When sending to multiple recipients, each unique address will be counted as a secure Email. In the event that a Customer exceeds the number of permitted secure Emails in any month, BT shall be required to pay for additional Users accordingly. BT shall at its sole option raise additional invoices and/or make adjustments to subsequent invoices to cover charges for the increase in the number of Users on a pro-rata basis for the remaining part of the current invoicing period.

b) Emails routed through PBE are limited to a maximum size of fifty megabytes (50 MB) per Email when compressed.

c) The Email Latency service level in the Service Level Agreement shall not apply to PBE.

d) PBE ONLY OPERATES WHEN USED IN CONJUNCTION WITH THE BE AND EMAIL CC SERVICES AND CANNOT OPERATE AS A STANDALONE SERVICE. EACH INDIVIDUAL PBE USER MUST BE AN EMAIL CC USER.

6 US Encryption

THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT THE ENCRYPTION OF EMAILS VIA PBE WILL BE PERFORMED IN THE UNITED STATES AND THAT THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED TO EFFECT THE TRANSFER OF DATA. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT BT CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

7. General Terms and Conditions

THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT USE OF PBE IS ENTIRELY AT THE CUSTOMER'S CONTROL AND DISCRETION. PBE is intended to be used solely to enable Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). Use of encrypted services in some countries may be subject to legislation. The Customer is advised to always check relevant legislation prior to deploying PBE. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of PBE. Furthermore the Customer shall indemnify and hold BT harmless from any damages (including without limitation reasonable costs) that may be awarded to any third party as a result of the operation of PBE

Appendix 9

Boundary Encryption Service

1 Overview

BT's Boundary Encryption Service ("BE") provides encrypted communication channels which enable the Customer to form a secure private Email network (SPEN) with nominated partner organisations ("SPEN Partners"). This configuration is known as "Enforced" encryption.

Additionally, the Customer can also receive encrypted Emails sent opportunistically from organisations that have TLS-capable mail servers for which there is no Enforced encryption with the Customer if such organisations have TLS-capable mail servers. This configuration is known as "Opportunistic" encryption.

If the Customer has subscribed to BE but has not explicitly identified any SPEN Partners, the Customer can receive Email sent opportunistically inbound over TLS, and send Emails encrypted opportunistically outbound to non-SPEN Partner organisations.

The Customer may also configure its email servers for the "Secure Connection" model of BE, in which case:

Email exchanges between BT and Customer's Secure Connection mail servers shall be secured by TLS encryption. Whether onward routing will be performed in unencrypted or encrypted format will depend on:

a) Customer specified TLS enforcements; and,

b) destination server capability to receive Emails over Opportunistic TLS.

THE CUSTOMER ACKNOWLEDGES AND ACCEPTS THAT IF THE SECURE CONNECTION MODEL IS NOT APPLIED TO A PARTICULAR MAIL SERVER, CUSTOMER'S INBOUND AND OUTBOUND EMAILS ORIGINATING FROM OR RECEIVED BY THAT MAIL SERVER SHALL NOT BE SECURED BY TLS ENCRYPTION. ACCORDINGLY, THE RESELLER ACKNOWLEDGES AND ACCEPTS THAT A CUSTOMER SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA SUCH MAIL SERVERS AND DOES SO ENTIRELY AT ITS OWN RISK.

If the Customer is using BE in conjunction with the PBE Service, BT's recommended best practice is for the Customer to implement the Secure Connection model of BE on all its mail servers.

"Member" means the Customer and organisations with whom the Customer creates an encrypted network by utilising the Boundary Encryption Service.

2 Provisioning

BT will aim to provision BE orders and BE change requests within 4 weeks of the order / change request being accepted by BT provided that all required technical due diligence has been completed by the Customer.

In the event that BT is required to allocate additional technical resources to the provision of BE due to the Customer failing to perform the required technical due diligence, BT reserves the right to charge the Reseller additional professional services fees at the rate of £1500 per person per day.

3 Configuration

Customer will define SPEN Partners with whom it wishes to communicate securely by domain. SPEN Partners may be customers or non-customers of BE, however BT will not support SPEN Partners directly. Non-SPEN Partner organisations may receive Emails over Opportunistic Outbound TLS as described in 1 above should their mail servers support the receipt of encrypted mail.

BE is based on the standard 'SMTP over TLS' (Simple Mail Transfer Protocol over Transport Layer Security) ("STARTTLS").

Both Customer's and the SPEN Partner's mail server must support STARTTLS to enable use of BE.

BE is supported by selected Towers through which all STARTTLS Email will be routed. Accordingly, Customer nominates which of their domains are to utilise BE.

When utilising BE in conjunction with the signaturing system functionality of Email AS, BT recommends that the Customer includes in its Email AS approved senders list all its SPEN Partner domains. If this recommended best practice is not followed the Reseller recognises and accepts that in certain circumstances involving unavailability of the local signaturing system, Email may be redirected to a remote signaturing system via a public network.

4 Certificates and Authentication

Where the Customer originates a STARTTLS connection the accepting mail server must provide its certificate for authentication. If the accepting mail server wishes to authenticate the Service then BT will supply its client certificate for authentication. If the accepting mail server cannot authenticate the Email will be returned to the Customer.

Where an external mail server originates a STARTTLS connection, the Service will supply its server certificate for authentication, but will not insist on the external mail server supplying its client certificate for authentication.

The validation of any certificate is based upon the Certificate Authority that has signed the certificate. For each certificate submitted by a remote mail server as part of a STARTTLS connection, the Service will validate that a recognised Certificate Authority has signed the certificate. If a certificate cannot be validated against a recognised Certificate Authority the connection will be aborted and the Email will be returned to the sender.

5 Encryption Terms and Conditions

The Customer acknowledges and accepts that BT can take no responsibility for the failure of Customer or any third party (including without limitation any SPEN Partner) to fulfil their obligations with regard to registering certificates or for the timeliness or accuracy of such information.

The Customer acknowledges and accepts that BE is intended to be used solely to enable Customer to enforce an existing, effectively implemented acceptable computer use policy (or its equivalent). Use of encrypted services in some countries may be subject to legislation. The Customer is advised to always check relevant legislation prior to deploying the BE Service.

The Customer acknowledges and accepts that BT can accept no liability for any civil or criminal liability that may be incurred by Customer as a result of the operation of BE.

Appendix 10

Archive L Service

1 Overview

Archive L is the collective name for a number of archiving Services, as described below, to which the Customer may subscribe. All Services within the Archive L range are compatible with approved versions of on-premise Exchange servers and hosted Exchange services.

1.1 Email Personal Archive L

The Email Personal Archive L Service is an Internet-based email archiving service which is designed to give the Customer's individual Users access to their own personal email archives directly from Microsoft Outlook or Outlook Web Access (where supported) in order to find and restore lost or deleted emails.

Customer's inbound and outbound emails, including attachments, are captured in an online searchable repository (the "Personal Archive"), which Users can search to find lost or deleted emails.

Users can also access the Personal Archive from Microsoft Outlook, Outlook Web Access (where supported), IBM Lotus Notes, BlackBerry devices and through a browser-based, secure website.

Users can search the Personal Archive for specific emails and attachments in two ways: Quick Search and Advanced Search. The Advanced Search option gives Users the ability to customize their searches based on a variety of criteria, such as message keywords, to, from, subject, date(s), and attachment type.

If enabled, Users can compose, reply to and forward messages directly from Email Personal Archive L, as they would in Outlook or Notes.

Users can create custom searches, based on a variety of criteria (e.g. date range, email sender, attachment type, etc.) and then save them so Users can re-run them as needed.

Moving Customer's legacy email into the Personal Archive and removing local archives helps reclaim space on Customer's shared drives and email servers.

Customer's Personal Archive can be used to recover historical email if a computer or laptops are lost or stolen.

Customers can ingest PST files into Email Personal Archive L where the folder structure is optionally maintained upon initial ingestion.

1.2 Email Discovery Archive L

The Email Discovery Archive L Service is an Internet-based email archiving service designed to expedite legal discovery (e-discovery) requests, enforce email use policies and aid in mitigating data loss. Discovery Archive aids Customers in email preservation related to lawsuits/legal holds, and aids in protecting attorney-client privileged communications.

EmailDiscovery Archive L stores and indexes emails, attachments, and BlackBerry messages (SMS text, PIN-to-PIN, call log) in a centralized, online repository.

Customers can place legal holds on specific communications (based upon search criteria) to aid in safeguarding the Customer's staff or automated deletion policies from inadvertently deleting case-relevant emails. Administrators and reviewers can flag attorney-client privileged communications, which can be excluded from e-discovery requests.

Email Discovery Archive L search log captures the activities of reviewers, so administrators can conduct appropriate reviews.

Administrators have the ability to group Users based on custom criteria. Reviewers can then search across these groups.

Customers can search the contents of archived emails and attachments using a variety of search criteria, including to, from, date, subject, message body, message attachments and other message properties.

Customer's reviewers can efficiently navigate through search results, identify highlighted search terms and tag potentially harmful emails, so they are easily retrievable for further review.

Customers can tag emails related to a specific case or legal matter and then export emails into a third-party case management solution or other application for further review and analysis.

Customer's reviewers can create and save customized email searches based on Customer's email policies, and re-run them as necessary.

Customer's reviewers can set up policy alerts to notify them when an email meets "Saved Search" criteria (e.g., contains specific words or phrases).

1.3 Email Personal Archive for BlackBerry

The Email Personal Archive L for BlackBerry Service is an Internet-based service designed to allow the Customer's individual Users to access and search archived emails, attachments, SMS, PIN-to-PIN messages and call log files via their BlackBerry devices. Users can find and restore lost or deleted emails and continue to use their BlackBerry device to compose, reply to and send messages in real time even when the Customer's primary email server experiences an outage. Personal Archive L for BlackBerry is an optional add-on service to the Email Personal Archive L Service.

Email Personal Archive L for BlackBerry can be deployed by administrators to Users from a Blackberry Enterprise Server (BES) or by Users via Blackberry Desktop Manager.

Users can log into Personal Archive for BlackBerry by clicking on the icon displayed on the device's home screen.

When the User clicks on the application, a splash screen is displayed for three seconds and then the User is prompted for their user credentials.

After successful login, the User is directed to the Home Screen (i.e. List View screen) of Personal Archive.

From the List View (Mailbox) Screen, Users can perform a number of functions, including: composing new messages, reply to or forward emails, and conduct simple or advanced searches.

Users can find old, lost or deleted emails using simple or advanced searches of all messages and call log files stored in their Personal Archive and then restore these messages back to their inbox.

The User can enter text into the search box and press the search icon to start the search. Search results can be filtered based on "Date", "From" and "To."

The User can use their Personal Archive to compose, reply to and send messages even if the Customer's primary email platform (e.g., Microsoft Exchange) is unavailable.

1.4 Email Archive Import Service L

The Email Archive Import Service L is an Internet-based service designed to migrate and ingest existing legacy email data into the Customer's archive repository. The import service allows the Customer to then search their email archive (e.g., Personal Archive, Discovery Archive and Advisor Mail) including both ingested legacy email and new email streams.

The Email Archive Import Service L requires a customer to ship via S-FTP or secure courier email data in PST or EML file format.

The Customer can manually extract the data and provide it in PST or EML format or use the Email Archive Legacy Data Extraction Service L for automated extraction from supported repositories.

With the Customer's guidance, the Email Archive Import Service L assigns ownership to each message that has been located. Messages that cannot be directly assigned to a specific individual are archived into a "catchall" mailbox within the email archive.

All migration activity can be logged and audited to provide integrity of the Customer's Email records and maintain "chain of custody."

The Email Archive Import Service L involves active participation by the Customer to plan, analyze and execute an ingestion plan with minimal business disruption.

1.5 Email Continuity L

IF BT IS UNABLE TO ESTABLISH AN SMTP CONNECTION TO THE CUSTOMER, THE CUSTOMER'S EMAILS WILL BE ROUTED TO THE EMAIL CONTINUITY L SERVICE ON BEHALF OF CUSTOMER ("CONTINUITY EVENT"). FOR THE AVOIDANCE OF DOUBT: (I) IF THE CUSTOMER'S FIREWALL ACTS AS A PROXY AND RESPONDS ON BEHALF OF THE MAIL SERVER, OR (II) IF THE CUSTOMER'S MAIL SERVER ISSUES ANY RESPONSE (INCLUDING WITHOUT LIMITATION ERROR CODES), THIS WILL CONSTITUTE AN SMTP CONNECTION AND WILL NOT BE A CONTINUITY EVENT

.

During a Continuity Event, the Customer's individual Users can access their email via a dedicated folder in Microsoft Outlook® or a web-based User interface. The User can: (i) view up to ninety (90) days of historical email, including new emails sent and received during the Continuity Event; (ii) create, reply to and forward emails; and (iii) use common email tools such as spell checking, inserting attachments and rich formatting.

If Customer is an Email Continuity L subscriber only, Continuity Emails will be stored within such service for a period of ninety (90) days. If Customer has purchased an additional archiving service under this Email Archiving L Service description, Continuity Emails will be retained based on the retention period selected by Customer in such service.

Continuity Emails will be delivered to Customer's primary email server at the point such server again begins to accept emails, with the exception that any emails which have been queuing for more than seven (7) days will not be delivered, and the Customer must instead retrieve the emails from the continuity archive described in Clause 1.5.2 above.

The Email Continuity L Service utilizes an opportunistic, rather than an enforced, transport layer security ("TLS") connection when attempting e-mail delivery. TLS is an enhanced security protocol designed to protect/encrypt e-mail during transport over the Internet. ALL BOUNDARY ENCRYPTION AND POLICY BASED ENCRYPTION CUSTOMERS ALSO SELECTING THE EMAIL CONTINUITY L SERVICE ACKNOWLEDGE AND AGREE THAT A TLS CONNECTION WILL BE ATTEMPTED BUT MAY NOT BE ACHIEVED AND THUS SUCH EMAILS MAY NOT BE ENCRYPTED. ACCORDINGLY, CUSTOMER ACKNOWLEDGES THAT IT SHOULD NOT SEND OR RECEIVE SENSITIVE DATA VIA THE EMAIL CONTINUITY L SERVICE OR CUSTOMER DOES SO ENTIRELY AT ITS OWN RISK.

The Email Continuity L Service only delivers email to a single nominated server per specified domain and "per User routing" Customers hereby accept this aspect of the service. Customer agrees to configure the Email Continuity L Service as a failover delivery route with the ClientNet interface and to further inform MessageLabs of the delivery location (mailhost name or ip address) by domain of its mail servers at commencement of this service. Customer acknowledges and agrees that it has an ongoing obligation to update BT during the Email Continuity L Service of any changes to such delivery location. Customer acknowledges that Customer's failure to make such configurations or to provide BT with such delivery information will adversely impact the functionality of the Email Continuity L Service.

2 General Terms and Conditions

BT emphasises that the configuration and use of the Service is entirely in the control of the Customer. BT recommends that the Customer has an acceptable computer use policy (or its equivalent) in place. In certain countries it may be necessary to obtain the consent of individual personnel. BT advises the Customer to always check its local legislation prior to deploying the Service. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation of the Service.

THE CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA AND THAT THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED TO EFFECT THE TRANSFER OF DATA. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT BT CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

The Customer acknowledges and agrees that (i) the scanning services (Email AV, Email AS, Email IC and Email CC) do not scan all emails that originally enter the archive and (ii) the scanning services (Email AV, Email AS, Email IC and Email CC) do not scan emails that are released from the archive for reinstatement to a User's mailbox. Accordingly, BT cannot be responsible for any virus, spam, images or inappropriate content that such reinstated emails may contain, and furthermore, the Service Level Agreement shall not apply to such reinstated emails.

Subject to the terms and conditions of this Agreement, BT grants Customer the non-exclusive, non-transferable right to install and use any software appurtenant to the aforementioned Services as applicable solely for the Customer's own internal business operations. All intellectual property rights in this software are and shall remain the property of BT(and/or its suppliers). Such software is licensed by BT, not sold. The Customer acknowledges that the software and all related information, including without limitation updates, are proprietary to BT and its suppliers. The Customer shall be responsible and fully liable for each User's compliance with or breach of the terms of this Agreement. The Customer shall immediately notify BT of any unauthorized use or violation of terms of this license.

The Customer acknowledges and agrees that MessageLabs cannot act as a third party downloader in any event for the purposes of SEC regulations.

Appendix 11

Smart Connect.cloud Service

1. Overview

Once the roaming user agent is installed and relevant configuration changes are made, requests for Web pages and attachments are electronically routed via the user agent to the URL Filtering Service ("Web v2 URL") and Web Anti Spyware

and Anti-Virus Service ("Web v2 Protect") and digitally examined.

2. **Service Description**

When the user connects to the Internet in designated 'in service' countries, the Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the Web v2 URL and Web v2 Protect service offerings.

3. **Configuration**

3.1. The configuration settings required to direct this external web traffic to the roaming user agent software, as well as forward traffic outbound to the Web v2 URL and Web v2 Protect services, are made and maintained by the Customer and are dependent on the Customer's technical infrastructure. The Customer must install a PAC file onto the User's PC so that the browser is pointed to the roaming agent when the browser is started up. A PAC file template can be downloaded from ClientNet and modified by the Customer. The Customer should ensure that internal HTTP/FTP-over-HTTP traffic (e.g. to the corporate intranet) is not directed to the roaming agent software.

3.2. Access to the Web v2 URL and Web v2 Protect is restricted to authorised systems that contain a valid version of the customer roaming agent software, as well as authorised users who are activated for these services in ClientNet. The roaming software agent and authorised user information is used to identify the Customer and dynamically select customer-specific settings.

3.3. Policy rules for the Web v2 URL service and content scanning for the Web v2 Protect service will be the same when a user is using the roaming agent service as when connected via a configured network location, i.e. corporate LAN.

3.4. The Customer acknowledges that the roaming agent will be provisioned with default settings applied from the outset which includes using reasonable endeavours to route the user's web traffic to an 'optimal' service infrastructure access point. This routing is based on an understanding of the roaming user's location based on IP address and use of a third party geo-location database to identify the likely country that the user is currently connecting from. BT will route users with the appropriate country designation to what is believed to be the optimal service access point for the specified country. This will be done independently of any assessment of the likely performance for the individual end user's connection and only for those countries which BT has deemed capable of providing an acceptable level of service.

For any other country outside of the acceptable service countries, the customer acknowledges that BT will not be able to provide the Web v2 URL or Web v2 Protect service capabilities. In these situations upon determining that the end user is located in a 'non-service' country, the roaming agent will 'fail open' such that the end user will be able to connect to the internet without the benefits of the BT service offerings that are available in acceptable service countries.

THE CUSTOMER ACKNOWLEDGES AND AGREES THAT THE USER'S WEB TRAFFIC MAY BE DIRECTED TO INFRASTRUCTURE LOCATED IN A GEOGRAPHIC LOCATION OUTSIDE THE EU FOR PROCESSING IN ACCORDANCE WITH THIS CLAUSE 3.4. THE CUSTOMER IS RESPONSIBLE FOR OBTAINING ALL CONSENTS AND APPROVALS REQUIRED FOR THE TRANSFER OF SUCH WEB TRAFFIC. ALL SUCH CONSENTS AND APPROVALS SHALL BE TAKEN BY CUSTOMER AT ITS OWN COST. THE CUSTOMER FURTHER ACKOWLEDGES AND AGREES THAT BT CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.

4. **Additional Export Terms for Smart Connect.cloud**

4.1 The Customer shall not, and shall not permit any third party to, sell, resell, export, re-export, transfer, divert, distribute, dispose of, disclose or otherwise deal with the Controlled Technology, directly or indirectly, to any of the following countries: Afghanistan, Angola, Armenia, Azerbaijan, Bosnia and Herzegovina, Burma, Burundi, China, Cuba, Democratic Republic of Congo, Eritrea, Ethiopia, Iran, Iraq, North Korea, Liberia, Libya, Nigeria, Rwanda, Sierra Leone, Somalia, Sudan, Syria, Tanzania, Uganda and Zimbabwe.

4.2 The Customer shall not transfer the Web Roaming Agent to any other company, or to any individual that is not an employee of the Customer except that: (i) The Customer may transfer to or enable the download of the Web Roaming Agent by its third party subcontractors for use on the Customer's behalf; and/or (ii) the Customer may transfer to or enable the download of the Web Roaming Agent by its third party end customers to whom it resells the BT Service, provided that the Customer makes such third parties aware of the obligations in this Clause.

Appendix 12
Instant Messaging Security.cloud Service (IMSS)

1 Overview

1.1 The Customer is required to synchronize its user directory with BT in order to create a list of Active Directory usernames and corresponding instant message (IM) usernames within ClientNet. An "Internal User" is a user known to the Customer's directory and uploaded into the IMSS administrative interface. An "External User" is a user unknown to the Customer's directory and/or not uploaded into the IMSS administrative interface.

1.2 The Customer is also required to make basic firewall changes to direct its IM conversations via BT.

1.3 Once IMSS has been configured in accordance with Clauses 1.1 and 1.2 above, IMs passing from Internal Users to External Users and vice versa are directed through IMSS for scanning by leading products including a heuristic scanner, Skeptic™.

1.4 IMSS is only able to scan certain versions of public IM clients. BT shall publish a list of supported versions of public IM clients on ClientNet. The Customer acknowledges and accepts that BT may update and change this list on a regular basis without notice.

1.5 If an incoming IM:
1.5.1 is deemed to contain a Virus or other malicious code, it shall be blocked;
1.5.2 contains a URL for a webpage where a Virus or other malicious code has been detected, access to such webpage shall be denied.

1.6 IMSS also provides basic anti-Phishing functionality which will block incoming IMs deemed to be Phishing attacks.

1.7 IMSS is able to scan certain versions of Word, Excel and PowerPoint documents, but not other attachments.

1.8 IMSS is unable to scan encrypted IMs.

2. Reserved.

3. IMSS Content Control

3.1 IMSS allows the Customer to configure its own rule based content filtering strategy for incoming and outgoing IMs.

3.2 The Customer is responsible for implementing the configuration options in line with the Customer's acceptable computer use policy (or equivalent) via ClientNet. Rules may be configured on a group or individual basis. Changes made to the rules by the Customer shall become effective within four (4) hours.

3.3 Options are available for defining the action to be taken upon detecting controlled content within an IM. These options are detailed on ClientNet and in the current version of the Administrator's Guide.

3.4 The Customer can review the results of its rules via ClientNet in the form of daily, weekly, monthly and annual summaries organised both by rule and by User.

4 Logs and Storage

4.1 If the Customer has enabled the logging functionality, BT shall compile daily logs of IMs scanned. Each log shall include date and time stamps, content, and names of files transferred. Any logs that are unable to pass to the Customer shall be stored for a period of thirty-one (31) days and then destroyed.

4.2 The Customer may also configure IMSS to send a copy of each IM to the Customer's compatible archive or storage solution.

5 Notifications

5.1 The Customer may configure IMSS to send an automatic notification:

5.1.1 to the sender and intended recipient in the event that an IM is blocked because it is deemed to contain a Virus, Phishing attack or controlled content; or

5.1.2 to the recipient if access to a webpage is denied because it is deemed to contain a Virus or malicious content.

5.2 The Customer can activate, customise and deactivate notifications using ClientNet.

6 Support

6.1 Support includes:

6.1.1 Walk through of the IMSS interface including a service description and Q&A session. (This does not include assistance with the set up of rules or analysis of the effectiveness of rules);

6.1.2Administrator's Guide;

6.1.3User Guide.

7 IMSS Terms and Conditions

7.1 Suggested content control word lists and template rules supplied by BT contain words which may be considered offensive. Customer accepts and agrees that BT may compile and publish default word lists using words obtained from the Customers' custom word lists.

7.2 The Customer acknowledges that IMs may contain personally identifiable information and that the logging and interception of IMs may therefore constitute the processing of personal data. Furthermore, the Customer acknowledges that IMSS is a configurable service and that the Customer is solely responsible for configuring IMSS in accordance with the Customer's acceptable computer use policy (or equivalent) and all applicable laws or regulations. Accordingly, BT advises the Customer to always check local legislation prior to deploying IMSS, and to ensure that it, and all its employees, are aware of and comply with any responsibilities they have in respect of data protection and privacy laws and/or regulations in connection with the Customer's use of IMSS. In certain countries it may be necessary to obtain the consent of individual personnel prior to the interception and logging of IMs. At a minimum, the Customer shall implement, with reasonable and minimal customisation, BT's default notification for IMSS to those who use any communications system covered by IMSS that (i) indicates that communications transmitted through such system will be logged and may be intercepted, (ii) indicates the purposes of such logging and interception, and (iii) obtains prior user consent to any such logging and interception. The Customer may translate but shall not otherwise modify any language relating to items (i), (ii) and (iii) in the preceding sentence as part of any customisation to the default notification for IMSS. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the Customer's operation of IMSS. The Customer shall hold BT harmless from any claims from its employees, any third party and/or governmental agencies relating to the interception or logging of IMs by BT or the Customer's failure to comply with laws and/or regulations.

7.3 **THE CUSTOMER'S ATTENTION IS DRAWN TO THE FACT THAT IMS PASSING THROUGH IMSS MAY BE SCANNED AND STORED ON HARDWARE LOCATED IN THE UNITED STATES OF AMERICA. CONSEQUENTLY CUSTOMER AGREES TO TAKE ALL NECESSARY STEPS TO (I) INFORM ANY OF ITS EMPLOYEES, AGENTS AND CONTRACTORS AS WELL AS THIRD PARTIES WHO USE THE COMMUNICATION SYSTEM COVERED BY IMSS OF THE FACT THAT ANY INFORMATION, INCLUDING POSSIBLY PERSONALLY IDENTIFIABLE INFORMATION OF INDIVIDUALS, PASSING THROUGH IMSS MAY BE PROCESSED IN THE UNITED STATES OF AMERICA; AND (II) OBTAIN SUCH EMPLOYEES, AGENTS, CONTRACTORS AND THIRD PARTIES' CONSENT TO SUCH PROCESSING PRIOR TO OR CONTEMPORANEOUSLY WITH THE OPERATION OF IMSS BY CUSTOMER. FURTHERMORE, ANY PERSONAL DATA THAT THE CUSTOMER PROVIDES TO BT MAY BE TRANSFERRED TO AFFILIATES OF BT AND/OR SUBCONTRACTORS ACTING ON BEHALF OF MESSAGELABS. SUCH AFFILIATES OR SUBCONTRACTORS MAY BE SITUATED IN THE UNITED STATES OR OTHER COUNTRIES THAT MAY HAVE LESS PROTECTIVE DATA PROTECTION LAWS THAN THE REGION IN WHICH THE CUSTOMER IS SITUATED, IN WHICH CASE BT WILL HAVE TAKEN STEPS SO THAT THE COLLECTED DATA, IF TRANSFERRED, RECEIVES AN ADEQUATE LEVEL OF PROTECTION. CUSTOMER AGREES TO TAKE ALL NECESSARY STEPS TO (I) INFORM ANY AND ALL OF ITS EMPLOYEES, AGENTS AND CONTRACTORS AS WELL AS THIRD PARTIES WHOSE PERSONAL DATA CUSTOMER PROVIDES TO BT OF THE FACT THAT THEIR DATA MAY BE PROCESSED IN THOSE COUNTRIES; AND (II) OBTAIN SUCH EMPLOYEES, AGENTS, CONTRACTORS AND THIRD PARTIES' CONSENT TO SUCH PROCESSING. BT CANNOT ACCEPT ANY RESPONSIBILITY FOR ANY CORRESPONDING BREACH OF APPLICABLE LEGISLATION OR REGULATIONS.**

NO SOFTWARE OR SERVICE CAN GUARANTEE A 100% IM DETECTION RATE AND THEREFORE BT CAN ACCEPT NO LIABILITY FOR ANY LOSS OR DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM ANY FAILURE OF IMSS TO DETECT SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT, OR FOR IMSS WRONGLY IDENTIFYING IM AS CONTAINING SPIM, VIRUSES, PHISHING ATTACKS, MALICIOUS CODE, BLOCKED URLs OR CONTROLLED CONTENT. Furthermore, the configuration of IMSS content control rules is entirely under the control of the Customer and the accuracy of such configuration will affect the accuracy of IMSS.