Security Services

Schedule to the General Terms

Contents

Security Options (Marketed as Assure Managed Security Services)

Where the Customer selects a security option as detailed in the Order, the following additional conditions shall apply:

1. General

1.1. BT's Managed Security Services (MSS) provide network protection and optimisation at a Customer Site. A range of security options are available. Typically these Services control inbound and outbound access to the Internet, performing functions that may include control of inbound traffic according to tightly controlled exceptions (Firewall), managing Users' outbound web access according to pre-defined policy (URL filtering), and scanning traffic to block viruses (anti-virus). The Customer acknowledges that the Service cannot ensure prevention or detection of all threats and unauthorised actions.

1.2. Customer Security Policy (CSP) Change Requests

1.2.1. BT will make reasonable endeavours to identify potential unforeseen consequences of Customer-requested CSP changes, and to advise the Customer accordingly. "Customer Security Policy" ("**CSP**") means the rules that are set and owned by the Customer, that dictate the operation of the Service. In order to be able to provide the Service BT has to know and accept these rules. BT will refer incorrectly specified CSP changes back to the Customer.

1.2.2. Occasionally BT may identify urgent security issues, such as identification by suppliers of urgent security risks or threats, or identification of a Security breach, that may affect the Customer. These may require BT to undertake Service maintenance or make changes to the Customer Security Policy. In such cases, BT will contact the Customer and obtain the Customer's agreement, before implementing such changes. BT will not be liable in any way for any problems caused by the Customer's failure, delay or refusal to agree to any such changes.

1.2.3. However, paragraph 1.2.2 above does not affect BT's rights as defined elsewhere in this Contract to maintain the integrity of its network, where issues may be affecting service to other customers.

1.3. Customer UserIDs and Passwords

1.3.1. The Customer may request up to five (5) login/password combinations for access to BT's online system, for use by the Customer or its Users. At the Customer's sole discretion, the Customer may assign one (1) login combination to BT personnel. The Customer is responsible for its Users' use of these IDs.

1.4. Customer Security Policy (CSP)

1.4.1. The Customer is responsible for providing BT with its CSP, on the template provided by BT. The CSP sets out the security "rules" that the Service will implement, and as such must be a clear and accurate definition of the Customer's requirements. The rules are statements that allow or prohibit connections between originating and destination addresses, for one or more TCP/IP services.

1.4.2. The CSP must be submitted at least twenty (20) Business Days before Contractual Delivery Date (CDD). BT will respond with a Security Policy Document, which must in turn be authorised by the Customer at least ten (10) Business Days before CDD.

1.4.3. CSPs can be complex to define, so BT consultancy is available to help capture the Customer's requirements. If the Customer orders this (chargeable) option, BT will capture the necessary information in consultation with the Customer Contact, and will produce the necessary CSP.

1.4.4. In no event shall BT be liable for any consequences arising from a mis-specification of the Customer's security requirements in the CSP, or from unforeseen consequences of a correctly specified and correctly implemented CSP.

1.4.5. BT will only retain log information for a limited time, after which time it will be destroyed.

1.4.6. The Customer is responsible for providing BT written notification of any changes (technical or business) that affect the security policy of any device that BT manages on behalf of the Customer.

1.4.7. The Customer will require a minimum of 512k outbound bandwidth to the BT Security Operation Centre for each managed appliance.

1.4.8. The Customer must not take any steps to access or modify any hardware or Software provided by BT.

1.4.9. De-installation charges will be equal to any prevailing rates for installation.

1.5. Software Application and Device Licences

1.5.1. BT will seek to validate that the Customer has ordered the correct number of licenses to serve its requirements, in accordance with vendor commercial terms and according to information provided by the Customer. If BT determines that the Customer has not ordered sufficient licences, BT will notify the Customer and the Customer must seek to rectify the situation within thirty (30) days. If the situation is not resolved within this time BT reserves the right to suspend Service. In any event, BT is not liable for undetected breaches of vendor commercial terms, where BT is acting on information provided by the Customer.

1.6. MSS SMB

1.6.1. BT's responsibility under this Contract for Managed Security Services is limited to the Firewall and any other CPE that may be provided as part of the solution.

1.7. The terms of this general paragraph do not apply to the Radius Authentication Service and the Radius/ACE Strong Authentication Service.

2. Managed Firewall Service

Service Options

2.1. VPN and IP Sec Service Configuration

2.1.1. This Service option provides secure connections between Customer Sites, usually over the Internet. IPSec tunnels are set up between Firewalls (that have been provided to the Customer as part of the BT Managed Firewall Service). This enables the Customer to use the public Internet as a secure extension to their network.

2.1.2. BT will support IP Sec Encrypted VPN tunnels for use with either:

(a) VPN IP Sec Remote - using Checkpoint SecuRemote, Secure or Cisco VPN Client;

(b) VPN IP Sec Site to Site, connecting BT Managed Firewall Service to BT Managed Firewall Service; or

(c) VPN IP Sec Extranet, connecting BT Firewall to 3rd party Firewall or Routers.

2.1.3. The CPE to support IPSec Encryption will be supplied as per the Equipment Schedule.

2.2. Next Generation Firewall Features

2.2.1. Customers may select optional services to be deployed on their BT Managed Firewall, depending on the Firewall model. BT will configure these services in accordance with the chosen tier of service (where applicable), and within the limitations of the Third Party Software used to deliver the service. The Customer acknowledges that BT cannot guarantee that this software will operate without fault or interruption or, in particular, to intercept or disarm all malware.

2.3. Firewall Intrusion Detection and Prevention Service

2.3.1. Traffic passing through the Customer's Firewall will be constantly monitored for attacks, in accordance with the applicable intrusion signature files. The initial Service will be implemented with a default configuration setting. The Service includes subscription to the necessary signature updates, which will be implemented upon release by the supplier. BT will not be responsible for evaluating these signatures beforehand and its remedy in the event of conflict with legitimate Customer traffic shall be to disable the appropriate signature (where possible).

2.3.2. For Bronze level services, no monitoring, alerting or service specific reporting shall be provided. The intent is to automatically block high impact / high confidence attacks, as defined by the supplier of the Software used to deliver the service. It will not be possible to add additional blocks to this vendor-defined signature list.

2.3.3. For Platinum services, BT will provide 24x7 monitoring of IPS alerts, and categorise the alarm according to its severity. In the event that a high priority threat is discovered, BT will use reasonable endeavours to notify the Customer as soon as reasonably practicable. The customer will be able to request BT to block traffic containing this threat, BT will not pro-actively initiate such a block without the Customer's express request. BT will provide incident reports as part of the Service, these will be available via an on-line portal.

2.4. Firewall URL Filtering Service

2.4.1. This Service element allows the Customer to block access to Internet sites which it deems to be undesirable. The Blacklisting capability organises Internet sites into groupings and the Customer may choose to block access to any or all groups.

2.4.2. The Customer will provide BT with details of the groups to which it wishes to block access and BT will configure the BT Equipment to reflect the specified policy. In the event of any change in the Customer's policy, BT will implement alterations in the configuration of the Service as soon as reasonably practicable. Additionally, as part of this Service option, BT will remotely download upgrades to the Blacklisting Software if such upgrades are, in BT's opinion, operationally necessary or as otherwise agreed between the Customer and BT.

2.5. Firewall Anti-Virus Service

2.5.1. This Service provides the Customer with anti-virus checking for web browser (http), and secure web browser (https) traffic. When the Customer requests an executable file from a site on the Internet, the file is inspected against the current antivirus definition file loaded on the server and, if no virus is detected, the file is passed to the Customer. If a virus is detected, the file will be blocked and deleted. Antivirus definition files are kept up to date by regular downloads direct from the antivirus servers. The Service is subject to maximum file size and compressed archive limits. Within these limits, the Customer can specify a maximum file size to be scanned.

2.6. DMZ Management

2.6.1. This Service option provides configuration of a Customer defined DMZ (demilitarized zone). Each Firewall has a base DMZ capacity with options for more to be added. Charges are made according to the total number of DMZs configured for the Customer's use.

3. Web Access Security

Service Options

3.1. Web Access Security SG URL Filtering

3.1.1. This Service element allows the Customer to block access to Internet sites which it deems to be undesirable. The Blacklisting capability organises Internet sites into groupings and the Customer may choose to block access to any or all groups.

3.1.2. The Customer will provide BT with details of the groups to which it wishes to block access and BT will configure the BT Equipment to reflect the specified policy. In the event of any change in the Customer's policy, BT will implement alterations in the configuration of the Service as soon as reasonably practicable. Additionally, as part of this Service option, BT will remotely download upgrades to the Blacklisting Software if such upgrades are, in BT's opinion, operationally necessary or as otherwise agreed between the Customer and BT.

3.1.3. The Customer acknowledges that this Service element is implemented using Third Party proprietary Software which will offer only the functions described by the supplier of that Software and cannot be guaranteed to operate without fault or interruption. BT will supply and operate a server(s) loaded with suitable Software which will constitute BT Equipment.

3.2. Web Access Security SG IM Control

3.2.1. This Service provides the Customer with the ability to enable Instant Messenger (IM) communications via the most common clients. The Service allows the Customer to control the IM communications by providing the ability to set limits on bandwidth used by IM, the ability to transfer files and issue warning text to Users.

3.3. Web Access Security SG Media Streaming Control

3.3.1. This Service provides the Customer with the ability to control the effect of streaming media on its bandwidth by allowing the Customer to limit access to such Services to specified Users, limiting the bandwidth available and allowing only set formats pre-selected by the Customer.

3.4. Web Access Security Bandwidth Optimisation

3.4.1. This Service allows the Customer to classify, control and if required limit the amount of bandwidth used by different classes of network traffic which is destined for single or multiple devices.

3.5. Web Access Security – Web Anti-Virus

3.5.1. This Service provides the Customer with anti-virus checking for web browser (http), secure web browser (https) and file transfer using the ftp protocol. When the Customer requests an executable file from a site on the Internet, the file is inspected against the current antivirus definition file loaded on the server and, if no virus is detected, the file is passed to the Customer. If a virus is detected, the file will be blocked and deleted. Antivirus definition files are kept up to date by regular downloads direct from the antivirus servers. This Service is only available as an optional addition to the Blacklisting Service. The Service is subject to maximum file size and compressed archive limits. Within these limits, the Customer can specify a maximum file size to be scanned.

3.5.2. The Customer acknowledges that this Service element is implemented using Third Party proprietary Software which will offer only the functions described by the Third Party supplier and cannot be guaranteed to operate without fault or interruption or, in particular, to intercept or disarm all viruses. BT will supply and operate a server(s) loaded with suitable Software which will constitute BT Equipment.

4. BT Messagescan

4.1. This Service provides internet-level Email and Web security to Customers who are permanently connected to the Internet with a fixed IP address. It cannot be provided to Customers with Email systems connected to the Internet via dial-up or ISDN lines or whose IP address is dynamically allocated.

4.2. The Service consists of the following components, some or all of which may be ordered:

4.2.1. BT MessageScan Email Anti-Virus Service (Email AV);

4.2.2. BT MessageScan Email Anti-Spam Service (Email AS);

4.2.3. BT MessageScan Email Image Control Service (Email IC);

4.2.4. BT MessageScan Email Content Control Service (Email CC);

4.2.5. BT MessageScan Web Anti-Virus and AntiSpyware Service (Web AVAS); and

4.2.6. BT MessageScan Web URL Filtering Service (Web URL).

4.3. Some or all of these components may be ordered under the following Service bundles:

4.3.1. BT MessageScan Email Protect (Email AV and Email AS);

4.3.2. BT MessageScan Email Safeguard (Email AV, Email AS, Email IC and Email CC);

4.3.3. BT MessageScan Web Protect (Web AVAS);

4.3.4. BT MessageScan Web Control (Web URL); and

4.3.5. BT MessageScan Web Protect and Control (Web AVAS and Web URL).

Service Components

4.4. BT MessageScan Email Anti-Virus service ("Email AV")

4.4.1. The Customer's inbound and outbound Email including all attachments, macros or executables are electronically routed via BT's scanning Towers and digitally examined by multiple industry leading anti-virus products and proprietary technology.

4.4.2. If Email or attachments are found to contain a Virus, an automatic alert may, if selected by the Customer, be despatched to:

(a) the sender and intended recipient (for inbound Email);

(b) the sender (for outbound Email); or

(c) an Email administrator (inbound and outbound Email).

4.4.3. The infected Email will be forwarded to a secure server pending automatic destruction after seven (7) days, unless it is transported as a mass mailer virus, in which case it will be deleted immediately.

4.4.4. 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 on ClientNet. If addresses are group Email names or aliases the Email will be released to all addressees in the group or alias.

4.4.5. BT will only forward Virus-infected Emails to the Customer. Virus-infected Emails will not be returned to the sender or forwarded to third parties. BT will release a Virus-infected Email within eight (8) normal working hours of receipt of a release request.

4.4.6. 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.

4.5. BT MessageScan Email Anti-Spam service ("Email AS")

4.5.1. The Service is designed to protect the Customer from unsolicited or unwanted Email. 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 on ClientNet.

4.5.2. The Customer may compile a private approved senders list or a private blocked senders list. A number of public blocked senders lists may also 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 options elected by the Customer.

4.5.3. 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 selected by the Customer. This action will supersede any less severe action previously allocated by any of the blocked senders list methods.

4.5.4. 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 selected by the Customer. This action will supersede any less severe action previously allocated by any of the preceding methods.

4.5.5. 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; or

(e) Spam Quarantine.

4.5.6. 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. 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.

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

4.5.8. 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 wrongly identifying an image as suspected to be 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.

4.6. BT MessageScan Email Image Control service ("Email IC")

4.6.1. The Customer's Email is scanned using Image Composition Analysis (ICA) to detect pornographic images contained in image files attached to Email. If an 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.

4.6.2. The Customer may specify the level of detection sensitivity as either High, Medium, or Low. The settings are subjective. Generally more images will be suspected to be pornographic at High sensitivity than at Low sensitivity.

4.5.3. If the Customer elects to redirect or delete Email containing a suspected pornographic image, then an automatic alert may, if selected by the Customer, be despatched to:

(a) the sender and intended recipient (for inbound Email);

(b) the sender (for outbound Email); or

(c) an Email administrator (inbound and outbound Email).

4.5.4. 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 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.

4.5.5. 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).

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

4.5.7. 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.

4.5.8. 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.

4.7. BT MessageScan Email Content Control ("Email CC")

4.7.1. The Service is designed to enable the Customer to configure his own rule based filtering strategy in line with his acceptable use policy (or its equivalent) for Email. 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. 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.

4.7.2. The options for defining the action to be taken upon detecting a suspected Email 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).

4.7.3. 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.

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

4.7.5. The Customer acknowledges 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.

4.7.6. 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.

4.8. BT MessageScan Web Anti Virus and AntiSpyware Service ("WebAVAS")

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

4.8.2. 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.

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

4.8.4. The Customer is responsible for setting and maintaining the configuration settings required to direct external traffic via the Service.

4.8.5. 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.

4.8.6. 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.

4.9. BT MessageScan Web URL Filtering Service ("WebURL")

4.9.1. The Customer's external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are electronically routed via the Web URL Filtering Service ("WebURL") and digitally examined.

4.9.2. The Customer is responsible for setting and maintaining the configuration settings required to direct external traffic via the Service.

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

4.9.4. 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 see an automatic alert Web page.

4.10. Additional terms for WebAVAS and WebURL

4.10.1. The Customer shall 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.

4.10.2. Access to the Service is restricted via Scanning IP (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.

4.10.3. 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.

4.10.4. 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 Web AVAS to detect viruses or spyware or for wrongly identifying viruses or spyware or 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:

(a) containing a virus; or

(b) constituting a blocked URL or containing blocked content,

except where such claim arises due to BT breach of contract or negligent act or omission.

4.11. Supply of the Service

4.11.1. 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.

4.11.2. 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 a material breach of the Contract.

4.11.3. 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.

4.11.4. 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. Any such installation, or part thereof, may not be dedicated to the sole use of the Customer.

4.11.5. If ordered, Email IC, Email AS and Content Control will be enabled for each of the Customer's domains. The Customer is responsible for setting the configuration options for Email IC, Email AS and Content Control for each domain using ClientNet.

4.11.6. BT emphasises that the configuration of the Service is entirely in the control of the Customer. The Services described are intended to be used solely to enable the Customer to enforce an existing, effectively implemented Acceptable Computer Use Policy (or its equivalent). 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.

4.11.7 BT will enable the Service. The Service Start Date occurs on the earlier of the Customer diverting mail to the Service or BT successfully sending a test message to the Customer.

4.12 Customer Responsibilities

4.12.1 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.

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

4.12.3 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.

4.12.4 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.

4.12.5 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 the implementation of any of the Services. BT can accept no liability for any civil or criminal liability that may be incurred by the Customer as a result of the operation the Services.

4.12.6 Any Customer data captured by BT in the delivery of this Service will remain the Customer's data and BT will only process this data to the extent necessary to deliver the Services or in accordance with the instructions of the Customer. At all times both parties will comply with their respective obligations under applicable data protection and privacy legislation.

5. Intrusion Prevention Service (IPS) - (Silver, Gold, Platinum Options)

5.1 The Intrusion Prevention Service provides protection against attacks on the Customer's network. BT will configure the Service in accordance with a policy defined and agreed with the Customer. BT shall provide the Service based on the technical and business information supplied by the Customer, or compiled by BT in collaboration with the Customer as part of the IPS Policy Production Service.

5.2 In the event that suspicious connections are identified an alarm will be raised. BT will analyse the cause of the alarm and categorise the alarm according to its severity. In response to an alarm, BT will use reasonable endeavours to comply with any arrangements agreed with the Customer and outlined in the incident response plan, but will take such action as it thinks appropriate in the circumstances, which may include disconnecting a device or dropping a connection in order to protect a Customer protected domain. BT will use reasonable endeavours to notify the Customer as soon as reasonably practicable of the occurrence of any alarm and the remedial action taken (if any).

5.3 Monitoring of the Intrusion Prevention device will be carried out twenty-four hours per day, seven days per week.

5.4. Where possible, BT will comply with actions outlined in the incident response plan. The actions taken by BT will depend on the options selected by the Customer. An incident response plan specifies the actions that BT will follow when an intrusion alert occurs on a Customer IPS sensor. The generated alert information can include source and destination IP of the attack, time when the attack occurred, sensor that detected the attack.

5.5. BT may remotely configure any CPE provided as part of this Service.

5.6. BT will provide reports as part of the Service, these will be provided via email.

5.7. BT will only retain log information for a limited time after which time, it will be destroyed.

5.8. The Customer is responsible for providing BT written notification of any changes (technical or business) that affect the security policy of any IPS Sensor that BT manages on behalf of the Customer.

5.9. The Customer will have minimum of 512k outbound bandwidth for the IPS Sensor to maintain connectivity to the BT Security Operation Centre and to collect alert information from the IPS Sensors.

5.10. The Customer must not take any steps to access or modify any hardware or Software provided by BT.

5.11. De-installation charges will be equal to any prevailing rates for installation.

5.12. The Customer acknowledges that this Service element is implemented using Third Party proprietary Software which will offer only the functions described by the supplier of that Software and cannot be guaranteed to operate without fault or interruption or, in particular, to intercept or disarm all viruses. BT will supply and operate the IPS sensors with suitable Software pre-loaded ready for configuration.

6. Radius Authentication

6.1. BT will provide use of the shared security server platform for the purposes of Radius Authentication for the number of User Sites as defined in the Order.

6.2. In order to provide an authentication facility, BT will provide and operate a shared security server platform, which will constitute BT Equipment. This platform will be configured with the appropriate information notified by the Customer to BT but the Customer acknowledges that such facilities cannot guarantee the detection or prevention of any unauthorised or unlawful access to the Service or to the Customer Network and accordingly BT accepts no liability for any such access.

7. Radius / ACE Strong Authentication

7.1. BT will provide use of the shared security server platform for the purposes of RSA Security SecurID authentication for the number of Users as detailed in the Order.

7.2. In order to provide an authentication facility, BT will provide and operate a shared security server platform, which will constitute BT Equipment. This platform will be configured with the appropriate information notified by the Customer to BT but the Customer acknowledges that such facilities cannot guarantee the detection or prevention of any unauthorised or unlawful access to the Service or to the Customer Network and accordingly BT accepts no liability for any such access.

7.3. BT will provide a security token and a Personal Identification Number, known as a PIN code, for each User. Unless the Customer has indicated in the Order that the Customer will carry out distribution of security tokens to Users, BT will distribute the tokens to Users, based on the information provided in accordance with paragraph 7.5 of this Service Schedule.

7.4. The security server facilities will make Users' access to the Customer Network subject to authentication of the User's identity in the following manner. When a User dials into an access server, a Point to Point Protocol session handshake will take place between the User's PC and the access server. The User must enter his/her user identification and PIN code, following which the access server will send an authentication request to the security server. Once the security server has validated the User's identity, through Remote Access the End User will be provided with addressing information and granted access to the Customer Network.

7.5. The Customer will provide BT with a Comma Separated Variable (CSV) file containing details of all Users. BT will provide a template for this.

7.6. Where the Customer is to carry out distribution of the tokens, BT will deliver the tokens, allocation details and User information to the address detailed in the Order. The Customer will be responsible for onward distribution of the token to the correct End User. In the event that End Users receive the incorrect token, BT reserves the right to raise additional Charges for any additional work required.

7.7. In all cases, the Customer will be responsible for the security and proper use of all security tokens and PIN codes and for the security of Users use of Service through their equipment. The Customer shall ensure that Users take all necessary steps to ensure that security tokens and PIN codes are kept confidential, secure, used properly and not disclosed or made available to unauthorised people. In particular, the Customer shall instruct End Users that security tokens and PIN codes should not be kept together, as this may enable security to be breached in the event of loss or theft.

7.8. In the event of loss or damage of a security token, it will be replaced by BT as a chargeable item.

7.9. The Charges for the Service include use of security tokens for up to three years from the Operational Service Date. Thereafter, the security tokens will need to be replaced and the charge for this will be subject to confirmation by BT at the appropriate time.

7.10. The Customer is responsible for the security of end devices (e.g. personal computers) when using this Service.

8. Secure Managed LAN

8.1. Service Overview

8.1.1. The Service provides enhanced Security for BT Managed LAN Services which is designed to prevent unauthorised access to the LAN as well as alerting Customers where unauthorised access attempts are detected.

8.1.2. The Service is designed to provide Customers with increased control of devices and Users that access their LAN, so as to mitigate security risks such as unauthorised collection of sensitive data or the introduction of Malware into the corporate network from unauthorised devices.

8.1.3. This Service is only available to Customers that have selected Proactive Alarm Monitoring or Proactive Fault Management.

8.1.4. The Service is provided for Cisco Managed Wired LAN Services only, it cannot be provided for Wireless LAN Services.

8.2. Service Options

8.2.1. The Service is available in 3 Service Options:

(a) Secure Ports - Static (Option 2);

(b) Secure Ports - MSAD (Option 3a); and

(c) Secure Ports RADIUS (Option 3b).

8.2.2. All options each comprise a bundle of Services that are combined to provide a comprehensive enhanced security Service. The Service(s) selected by the Customer is detailed on the Order. Changes to these may be initiated by the Customer during the life of this Contract via the BT change control process.

8.3. Secure Ports - Static (Option 2)

This option provides an enhanced access control Service for LANs used in a static environment ideal where devices remain on one LAN port or where devices are rarely changed on a particular LAN port.

This option includes the following Services:

8.3.1. Configure Secure Ports

As part of this Service additional security is provided by locking LAN ports to specific MAC addresses, so preventing non-approved devices from accessing the LAN. Configuration changes, including changing the MAC address associated with a LAN port, can only be implemented by BT on request. This work can be completed as part of the SMACs Service. This work must be requested by the Customer via the BT change control process and all such work will be subject to additional charges.

8.3.2. Security Event Management

As part of this Service BT will detect and handle security alarms which occur on Managed LAN devices. An alarm will be generated when a device with an unauthorised MAC Address attempts to access a port. The Managed LAN device is configured to automatically go into 'error disabled' mode which prevents access to the port by the unauthorised device. The alarm will be received and acted upon by the BT helpdesk. No security alarm detection Service 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 security alarm.

8.3.3. Enhanced Management Plane Access Control

This Service provides device administration such as device back-up and configuration. BT will use SSH to securely access managed LAN devices. SSH provides encryption for all communications with the device and therefore gives added security. BT will also build the Customer LAN network as a discrete entity on the BT network management authentication servers. This will give greater control over access to the Customer's devices. As part of this Service the Customer also has access to audit reports created from logs on the BT authentication servers. These logs will show successful & unsuccessful login attempts to their devices by BT staff. The reports can be accessed by the Customer from the Service Portal. Due to a limitation of the standard protocols used, not all accounting messages can be recorded.

8.3.4. LAN Security Software Update Advisory

BT will inform the Customer when a software upgrade to the Customer's LAN switch is deemed essential where notified by the switch vendor. Such upgrades will be necessary to resolve security vulnerabilities in the configuration deployed on the Customer's LAN switch. Should a software upgrade be necessary, the Customer is responsible for raising a change request via the BT change control process Software upgrades will be subject to additional charges unless the charges are covered by subscription to the CPE Software Upgrade Management Service.

8.4. Secure Ports - MSAD (Option 3a)

This option is an enhancement to the Secure Ports –– Static Option. It provides an enhanced access control Service for LANs used in a dynamic environment where devices are often moved around on the wired LAN or where there is a need to authenticate Users rather than LAN devices. This option is suitable where the Customer uses MSAD (Microsoft Active Directory) to authenticate users gaining access to their IT resources.

This option includes the following Services:

8.4.1. Configure Secure Ports

(a) Additional security is provided by configuring the 802.1X protocol/software on LAN ports. Where fixed devices don't support the 8021X protocol LAN ports will be locked to specific MAC addresses, so preventing non-approved devices from accessing the LAN. LAN ports are configured to authenticate device/user login via a RADIUS server. Two RADIUS servers are required for resilience. As part of the authentication process, the RADIUS servers forward authentication requests to the Customer's MSAD. The MSAD then authenticates the request, based on the User credentials it holds, and replies back to the RADIUS server. As part of this Service user accounts are contained within the Customer's MSAD, therefore the Customer is responsible for managing the MSAD and the User credentials.

(b) Installation and configuration of the 802.1X software agent on Customer devices such as laptops and computers is not provided as part of the Service. Supported 802.1X applications include Microsoft Vista & XP Service Pack 2, support of other applications is subject to BT agreement and maybe subject to additional charges.

(c) BT will work with the Customer, to integrate the RADIUS servers with the Customer's MSAD. The Customer is responsible for installing a software agent on a server in the MSAD domain. This agent will provide the interface between the RADIUS server and the MSAD. BT will provide the required documentation to support the installation of the RADIUS Server to the MSAD software agent. Once the software agent is installed, BT will work with the Customer to test that the BT supplied RADIUS servers, successfully integrate with the Customer MSAD via the software agent.

8.4.2. Security Event Management

Where non 802.1x LAN devices are locked to LAN ports by a fixed MAC address, BT will detect and handle security alarms which occur on those managed LAN devices. An alarm will be generated when a device with an unauthorised MAC Address attempts to access a port. The managed LAN device is configured to automatically go into 'error disabled' mode preventing access to the port. The alarm will be received and acted upon by the BT helpdesk. No security alarm detection Service 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 security alarm.

8.4.3. Enhanced Management Plane Access Control

(a) This Service provides device administration such as device back-up and configuration. BT will use SSH to securely access managed LAN devices. SSH provides encryption for all communications with the device and therefore gives added security. BT will also build the Customer LAN network as a discrete entity on the BT network management authentication servers. This will give greater control over access to the Customer's devices.

(b) As part of this Service the Customer also has access to audit reports created from logs on the BT authentication servers. These logs will show successful & unsuccessful login attempts to their devices by BT staff. The reports can be accessed by the Customer from the Service Portal. Due to a limitation of the standard protocols used, not all accounting messages can be recorded.

8.4.4. LAN Security Software Update Service

BT will inform the Customer when a software upgrade to the Customer's LAN switch is deemed essential where notified by the Switch vendor. Such upgrades will be necessary to resolve security vulnerabilities in the configuration deployed on the Customer's LAN switch. Should a software upgrade be necessary, the Customer is responsible for raising a change request via the BT change control process. Software upgrades will be subject to additional charges unless covered by subscription to the CPE Software Upgrade Management Service.

8.4.5. 802.1X configuration of User LAN Ports

User LAN ports are configured to use the 802.1X protocol to provide an authentication facility which authenticates Users trying to access the LAN. Supported 802.1X applications include Microsoft Vista & XP Service Pack 2. The Customer is responsible for supply & installation of any supported applications required on their devices. Active ports without Users such as printers will be configured to specific MAC addresses.

8.4.6. On-site RADIUS (proxy) authentication

The Service includes configuration of the Customer's RADIUS servers so to enable integration with the Customers MSAD. Once the required configuration is completed this will allow the RADIUS servers to forward authentication requests to the Customer's MSAD. This provides for a common set of user credentials and allows Customers to manage their own user credentials while maintaining a clear demarcation point for management of the LAN. The supply of the RADIUS Servers is subject to additional charges. The RADIUS Servers must be separately specified and ordered where required as part of the solution. BT recommends that the Customer orders Business Premium Care Maintenance and Proactive Alarm Monitoring for the RADIUS servers.

8.4.7. User Access Reporting (customer-generated)

Under the Secure Ports MSAD Option the Customer's MSAD server will generate reports on the user authentication requests made. The Customer can produce reports showing the User access request details by running these reports from the MSAD server.

8.4.8. RADIUS Security Software Update Advisory

BT will inform the Customer when a software upgrade to the RADIUS server software is deemed essential where notified by the server vendor. Such upgrades will be necessary to resolve security vulnerabilities in the configuration deployed on the Customer's RADIUS servers. Should a software upgrade be necessary, the Customer is responsible for raising a change request via the BT change control process. Software upgrades will be subject to additional charges.

8.4.9. RADIUS Configuration Verification

BT will carry out regular remote manual checks to confirm that key security aspects of the RADIUS server configuration have not been unexpectedly altered. If an unexpected change is detected, then BT will deal with this as a security event as detailed in the Security Event Management Service.

8.5. Secure Ports RADIUS (Option 3b).

This option provides an enhanced access control Service for LANs used in a dynamic environment where devices are often moved around on the wired LAN or where there is a need to authenticate Users rather than LAN devices. The Customer would select this option where a suitable MSAD does not exist or where the Customer would prefer BT to manage their LAN User accounts. User credentials for authenticating User access to the wired LAN are held and managed by BT on Radius Servers.

Formatted: Indent: Left: 1.75 cm

This option includes the following Services:

8.5.1. Configure Secure Ports

(a) Additional security is provided by configuring the 802.1X protocol/software on LAN ports. Where fixed devices do not support the 8021X protocol LAN ports will be locked to specific MAC addresses, so preventing non-approved devices from accessing the LAN. LAN ports are configured to authenticate device/user login via a RADIUS server. Two RADIUS servers are required for resilience. The RADIUS servers authenticate the Users using account and password information held in the RADIUS database. Administration of the RADIUS database is set up and managed by BT on the Customer's behalf.

(b) Installation and configuration of the 802.1X software agent on Customer devices such as laptops and computers is not provided as part of the Service. Supported 802.1X applications include Microsoft Vista & XP Service Pack 2, support of other applications is subject to BT agreement and maybe subject to additional charges.

8.5.2. Security Event Management

Where non 802.1x LAN devices are locked to LAN ports by a fixed MAC address, BT will detect and handle security alarms which occur on those managed LAN devices. An alarm will be generated when a device with an unauthorised MAC Address attempts to access a port. The Managed LAN device is configured to automatically go into 'error disabled' mode preventing access to the port. The alarm will be received and acted upon by the BT helpdesk. No security alarm detection Service 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 security alarm.

8.5.3. Enhanced Management Plane Access Control

(a) This Service provides device administration such as device back-up and configuration. BT will use SSH to securely access managed LAN devices. SSH provides encryption for all communications with the device and therefore gives added security. BT will also build the Customer LAN network as a discrete entity on the BT network management authentication servers. This will give greater control over access to the Customer's devices.

(b) As part of this Service the Customer also has access to audit reports created from logs on the BT authentication servers. These logs will show successful & unsuccessful login attempts to their devices by BT staff. The reports can be accessed by the Customer from the Service Portal. Due to a limitation of the standard protocols used, not all accounting messages can be recorded.

8.5.4. LAN Security Software Update Service

BT will inform the Customer when a software upgrade to the Customer's LAN switch is deemed essential where notified by the Switch vendor. Such upgrades will be necessary to resolve security vulnerabilities in the configuration deployed on the Customer's LAN switch. Should a software upgrade be necessary, the Customer is responsible for raising a change request via the BT change control process. Software upgrades will be subject to additional charges or may be covered by subscription to the CPE Software Upgrade Management Service.

8.5.5. 802.1X configuration of User LAN Ports

(a) User LAN ports are configured to use the 802.1X protocol to provide an authentication facility which authenticates Users trying to access the LAN.

(c) Supported 802.1X applications include Microsoft Vista and XP Service Pack 2. The Customer is responsible for supply and installation of any supported applications required on their devices. Active ports without Users such as printers will be configured to specific MAC addresses.

8.5.6. On-site RADIUS authentication

(a) BT will provide an authentication facility for users accessing the Customer LAN. The Service includes configuration of the Customer's RADIUS Server devices so to enable the RADIUS servers to authenticate requests against the User details stored. The configuration includes the initial loading of user account details as provided by the Customer. Subsequent changes to the account details must be requested by the Customer via the BT change control process and will be subject to additional charges.

(b) As part of the Service all user credentials (e.g. username and password) will be held on the Customer sited RADIUS server and managed remotely by BT.

(c) The supply of the RADIUS Servers is subject to additional charges. The RADIUS Servers must be separately specified and ordered where required as part of the solution. BT recommends that the Customer orders Business Premium care Maintenance and Proactive Alarm Monitoring for the RADIUS servers.

8.5.7. User Access Reporting (Customer-generated)

BT will configure the RADIUS Servers to allow Customers to run reports which show User accesses to the LAN such as successful and unsuccessful login attempts to protected LAN ports. The Customer is responsible for providing their own web browser application such as Microsoft Internet Explorer to access the RADIUS servers for the purposes of running reports.

8.5.8. Database Management

BT will provide full management for all User accounts stored on the on-site RADIUS Servers including initial bulk creation of user accounts on installation. Key features of this Service include password management, suspension, deletion and reset of accounts. Once the initial configuration and installation of the Service is set up, further administration of User accounts must be requested by the Customer via the BT change control process and all such requests will be subject to additional charges. This work can be completed as part of the SMACs Service.

8.5.9. RADIUS Security Software Update Advisory

BT will inform the Customer when a software upgrade to the RADIUS server software is deemed essential where notified by the server vendor. Such upgrades will be necessary to resolve security vulnerabilities in the configuration deployed on the Customer's RADIUS servers. Should a software upgrade be necessary, the Customer is responsible for raising a change request via the BT change control process. Software upgrades will be subject to additional charges.

8.5.10. RADIUS Configuration Verification

BT will carry out regular remote manual checks to confirm that key security aspects of the RADIUS server configuration have not been unexpectedly altered. If an unexpected change is detected, then BT will deal with this as a security event as detailed in the Security Event Management Service.

8.6. Customer Responsibilities

8.6.1. The Customer is responsible for the physical security of any equipment provided as part of the Service which is located at Customer Sites.

8.6.2. The Customer is responsible for providing appropriate security awareness training for their employees.

8.6.3. The Customer is responsible for safeguarding of all sensitive information (including account details) provided to the Customer for the management of the Service.

9. Get VPN

9.1. Service Overview

9.1.1. The GET VPN Service is an encryption Service which provides an enhanced method of encrypting data transmitted over VPNs. The Service is designed to provide an increased level of data confidentiality and integrity for sensitive data while the data is in transit across the Customer's VPN.

9.1.2. As part of the Service, branch Site routers are configured as part of a group, in which group member Sites are authorised to exchange encrypted traffic. A centralised Key Server distributes the encryption keys to each member of the group via a protocol called Group Domain of Interpretation (GDOI). GDOI establishes security associations and provides encryption key management among authorised group members Sites. GDOI also periodically refreshes cryptographic keying information and distributes it to group members Sites.

9.1.3. The Service is only available to Customers that have selected Proactive Fault Management.

9.1.4. The Service is provided by a BT IL3 Accredited Service Centre.

9.2. Hosted Equipment

9.2.1. The Key Servers provided as part of the Customer's VPN must have the Hosted Equipment Service option. The Hosted Equipment Service provides the rack space, power and air conditioning necessary to host equipment within a BT IL3 Accredited Service Centre. Two Key Servers will be provided, Each Key Server will be located at separate BT IL3 Accredited Service Centres to provide protection against loss of Service.

9.3. Service Components

The Service comprises:

9.3.1. Encryption

An encryption overlay using FIPS 140-2 based encryption will be provided to give protection of data transmitted over the Customer's VPN. The encryption capability is an integral part of the WAN routers located at the Customer Sites. Where the Customer uses a router which is not FIPS 140-2 compliant or is currently undergoing FIPS 140-2 assessment the Customer acknowledges that the Service will be affected and accepts all associated security risks to data transmitted over the VPN.

Formatted: Indent: Left: 1.75 cm

9.3.2. Certificate Authority

The Service uses Digital Certificates to authenticate the Key Servers and routers at Customer Sites. The Digital Certificates are used to ensure only legitimate routers are used within the GET VPN Service. All Digital Certificates provided as part of the Service will be authenticated, issued and managed within a BT's IL3 Accredited Service Centre. The Digital Certificates will be issued with a maximum life of 1 year. Digital Certificates will be renewed before expiry and revoked if devices are replaced or cease to be part of the Service.

Formatted: Indent: Left: 1.75 cm

9.3.3. Key Management

Key management of the Service is performed by Key Servers as described in paragraph 9.1.2.

9.3.4. Proactive Incident Monitoring

In addition to the standard Proactive Fault Management Service, the GET VPN Service includes additional checks to ensure that the encryption features provided as part of the Service are functioning correctly. Where a fault is detected in the GET VPN Service, alarms are raised and corrective action will be taken in accordance with the terms of the Proactive Fault Management Service.

Formatted: Indent: Left: 1.75 cm

9.4. The Customer's Responsibilities

In addition to any other responsibilities defined elsewhere in this Contract, the Customer is also responsible for the following:

9.4.1. The Customer accepts and acknowledges that subsequent to the release of the CESG Information Assurance Notice (CIAN) 2010-05 issued by CESG, BT cannot provision the GET VPN Service to afford protection of data with a business impact level of 3-3-X (as defined in the HMG Information Assurance Standard 1 (IAS1)) without the Customer's accreditor accepting all potential security risks to data transmitted over the VPN. Therefore, the Customer is responsible for ensuring the Service is suitable for their needs and accepting all potential security risks to data transmitted over the VPN. For the avoidance of doubt, BT will have no liability to the Customer for a failure to achieve a business impact level of 3-3-X to provide confidentiality & integrity of data transmitted over the network.

9.4.2. The Customer is responsible for ensuring that any Customer Equipment and non–BT provided services connected and/or used with the Service are accredited to the same business impact level as the GET VPN Service.

10. Defined Terms

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

"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.

"Digital Certificate" means electronic credentials that are used to authenticate devices. **"Firewall"** means a hardware device together with any associated Software, designed to prevent unauthorised access to the Customer's LAN.

"GET VPN" means Group Encrypted Transport Virtual Private Network.

"Key Server" means a specially configured router which distributes encryption keys and security policy via a protocol called Group Domain of Interpretation (GDOI).

"Malware" means software programs designed to damage or do other unwanted actions to a computer system such as viruses, worms, trojan horses, and spyware.

"MSAD" means Microsoft Active Directory.

"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**".

"RADIUS" means remote authentication dial in user server.

"Spam" means unsolicited commercial Email.

"SSH" stands for Secure Shell and means a method of securely communicating with another computer.

"Tower" means a cluster of load balanced servers, configured to provide the Messagescan Services.

"Working Hours" means each hour within such times and on such days applicable to the level of CPE Maintenance.