# Our Customer Terms



Internet Direct and Business Broadband

## Part D – Mail and Web Protection / Mail and Web Control

## Contents

Click on the section that you are interested in.

# Part D – Mail and Web Protection / Mail and Web Control

# Part D – Mail and Web Protection / Mail and Web Control

# Part D – Mail and Web Protection / Mail and Web Control

Certain words are used with the specific meanings set out in this Mail and Web Protection/ Mail and Web Control section, Part A – General of the Internet Direct and Business Broadband sectionand in the General Terms of Our Customer Terms.

## 1 About this Part

1.1 This is part of the Internet Direct and Business Broadband section of Our Customer Terms. Provisions in other parts of the Internet Direct and Business Broadband section, as well as in the General Terms of Our Customer Terms, may apply to your Mail and Web Protection or Mail and Web Control service.

See clause 1 of the General Terms of Our Customer Terms for more detail on how the various sections of Our Customer Terms should be read together.

See clause 1 of Part A – General of the Internet Direct and Business Broadband section for more detail on how the various parts of the Internet Direct and Business Broadband section should be read together.

1.2 This part only applies if you have the Mail and Web Protection or the Mail and Web Control service.

1.3 If there is an inconsistency between this part and the other parts of the Internet Direct and Business Broadband section of Our Customer Terms, this part prevails to the extent of the inconsistency.

1.4 This Part D - Mail and Web Protection / Mail and Web Control of the Internet Direct and Business Broadband section of Our Customer Terms applies in respect of services acquired under this section prior to 1 July 2009. For services acquired on and from 1 July 2009, the Internet Solutions section of Our Customer Terms applies

## 2 Mail and Web Protection/ Mail and Web Control

**What are Mail and Web Protection and Mail and Web Control?**

2.1 Telstra's Mail and Web Protection ("**Protection**") and Mail and Web Control ("**Control**") service packages are email and web protection services for Telstra's business customers.

2.2 The Protection service package comprises the following services:

(a) an email anti virus service;

(b) an email anti spam service; and

(c) a web anti spyware and anti virus service.

2.3 The Control service package comprises the following services:

(a) an image control service;

(b) a content control service; and

(c) a web URL filtering service.

**Special requirements**

2.4 We will tell you of any restrictions or specific requirements that you will need to meet before we can provide the Protection or the Control services to you. These requirements are in addition to any requirements specified in this section of Our Customer Terms.

2.5 To receive the Protection or Control services, your email system or other relevant system must be permanently connected to the Internet with a fixed IP address.

2.6 We cannot provide the relevant Protection or Control service to you if your email system or other relevant system is connected to the Internet through dial-up or ISDN lines or where the IP address of your email system or other relevant system is dynamically allocated.

**Limitations in relation to Exchange Mail**

2.7 If you use either the Protection or Control services with our Exchange Mail service:

(a) you cannot use the outbound email scanning Protection or Control services with your Exchange Mail service; and

(b) emails sent between customers with an Exchange Mail service will not be filtered for spam by the Protection or Control services.

**Open Relay test**

2.8 We or our suppliers may, at any time, test whether your email system or other relevant system allows open relay. We will endeavour to give you reasonable notice before such testing occurs.

**Termination**

2.9 Either of us may terminate a Protection or Control service package by giving the other at least 30 days' written notice.

# Part D – Mail and Web Protection / Mail and Web Control

**Online service tool**

2.10 We will provide you with access to an online tool accessible through the Internet to configure, manage or request reports on the Protection and Control services. If required, we will provide you with a user identification and password to enable you to access this online tool.

2.11 We will endeavour to inform you of an emergency event or any maintenance that may materially affect a Protection or a Control service by posting an alert message on the online tool.

**Additional reporting**

2.12 We may provide user or group administration and reporting services with the relevant Protection or Control service.

2.13 To use these additional administration and reporting services, we may provide you with a software application (the "**client proxy**"). You must comply with the terms of any end user license agreement provided to you with the client proxy.

**Changes to delivery mechanism**

2.14 We can change any part of the Protection or the Control platform without telling you provided that it does not affect the Protection or the Control service. However, if such a change affects the Protection or the Control service, we will only do so in accordance with the variation process set out in the General Terms of Our Customer Terms.

**Planned maintenance**

2.15 We will endeavour to carry out planned maintenance without affecting the Protection or a Control services. If we are required to perform emergency maintenance on a Protection or a Control service, then we will endeavour to inform you as soon as possible.

**Email queue lengths**

2.16 We will endeavour to continuously monitor the email queue lengths. If we detect a rising email queue for your domain, then we will test for the ability of your receiving mail server to receive email and will endeavour to notify you if this test fails.

2.17 If we are unable to deliver email to you, then we will endeavour to store your inbound email for up to seven days. After this period, your emails will be deleted from our systems.

**No guarantee**

2.18 While this service is provided to you with reasonable care, due to technological limitations we do not promise that:

(a) all spam emails will be detected or that any email identified as spam is actually spam;

(b) all potential viruses and spyware will be detected or removed by the relevant service; and

(c) all content configured to be detected or pornographic images will be detected, or that any image detected as a pornographic image is actually pornographic in nature.

2.19 We and our external suppliers of the Protection and Control services are not responsible for any liability to any person resulting from:

(a) information passing through the Protection or Control services from you; and

(b) any delivery or non-delivery of an email, web page, image or other content,

where that liability is not directly or indirectly attributable to us or our external supplier's breach of these terms or negligent act or omission.

**Security threat**

2.20 If we reasonably suspect that the continued provision of a Protection or a Control service compromises or will compromise the security of the Protection or the Control service, for example due to hacking attempts or denial of service attacks, then we may temporarily suspend the provision of the service to you.

2.21 If we temporarily suspend your Protection or Control service, then we will inform you and work with you to resolve such issues so as to re-instate the service to you at the earliest opportunity.

**Termination by supplier**

2.22 If one of our external suppliers suspends or terminates a service we rely on to provide your Protection or Control service, then we may suspend or terminate your service after giving you at least 30 days notice or, if that is not possible, as much notice as is reasonably possible in the circumstances.

**Consequences of suspension or termination**

2.23 If we suspend or terminate a Protection or a Control service for any reason, then we will reverse all configuration changes made during the provisioning of that service. You are solely responsible for making all other necessary configuration changes to your mail servers and to inform your Internet service provider of the need to reroute inbound email.

**Intellectual property rights**

2.24 The intellectual property rights in the Protection and the Control services and any hardware or software used in connection with the services are and will at all times remain our property or that of our licensors or suppliers (as the case may be).

**Location of our hardware used to provide the services**

2.25 Subject to applicable law, we may provide a Protection or a Control service from any hardware installation anywhere in the world.

2.26 We do not promise that any installation or any part of it is dedicated to your sole use.

**General**

2.27 You acknowledge that in certain countries you may have to obtain the consent of each individual person to use the Protection or the Control service.

2.28 You are responsible for checking any local laws applicable to your use of the Protection or the Control service prior to obtaining the service from us.

2.29 We and our external suppliers do not accept any civil or criminal liability that may be incurred by you as a result of the operation of the Protection or the Control service or your use of the service.

## 3 Helpdesk

3.1 We will provide a help desk that is available 24 hours a day, 7 days a week. We will give you the details of the help desk, including the contact details when you request the Protection or Control service package.

3.2 You must report all faults with a Protection or a Control service to our help desk and give the details of the fault, and all other information necessary for us to investigate the fault.

3.3 If you report a fault with a Protection or a Control service to our help desk, then we will

determine its priority level and endeavour to respond as defined in the table below.

| Priority Level | Definition | Response target |
|---|---|---|
| Critical | Loss of service that cannot be circumvented | 95% of calls responded to within 2 hours |
| Major | Loss of service that can be circumvented, partial loss of service or service impairment | 85% of calls responded to within 4 hours |
| Minor | Potentially service affecting | 75% of calls responded to within 8 hours |
| Information | Non- service affecting information request | 65% of calls responded to within 24 hours |

## 4 Your obligations

4.1 You will provide us with all relevant information, including technical data, consents and all other information we may reasonably request from time to time to allow us to supply the Protection and Control services to you.

4.2 You agree that all information and data that you provide to us are complete and accurate.

4.3 You agree to:

(a) use the Protection or Control services for legitimate business purposes only;

(b) comply with all relevant laws (including all privacy laws), and not use the Protection or Control services for any unlawful purpose or in breach of any laws;

(c) comply with any reasonable directions we notify you in respect of your use of the Protection or the Control services;

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

(e) not re-sell, sub-lease, sub-rent or sub-license the Protection or the Control services to any other person, and must not allow any other person to use the services without our written consent;

(f) use all reasonable efforts to ensure that you inform (for example via a banner

message on emails) those who use any communications system covered by the Protection or the Control services, that communications transmitted through that system may be intercepted, and indicate the purposes of such interception;

(g) not use, or require us to use, any data obtained via the services for any unlawful purposes; and

(h) use the Protection or the Control services in a responsible manner and not allow your email systems to:

(i) act as an open relay;

(ii) send or receive bulk email where such bulk email was initiated by you; or

(iii) send spam.

4.4 If we find that your email systems allow open relay or can be used to send bulk email or spam, then we will inform you and may immediately suspend all or part of a Protection or a Control service until you rectify those issues to our satisfaction.

4.5 In addition to our termination rights, if you breach your obligations in this Mail and Web Protection / Mail and Web Control section of Our Customer Terms, then

(a) we may charge you for any remedial work (at our then current rates as notified by us to you at that time) which becomes necessary as a direct result of your breach; and

(b) we may suspend or terminate the relevant Protection or Control service until you provide a suitable undertaking and security in terms satisfactory to us that you will comply with your obligations.

## 5 Fees and charges generally

### Charges

5.1 We will charge you a monthly charge for the Protection and Control service packages as set out in the table below:

| Service package | Set up fee (once off) (GST excl.) | Maximum number of registered users | Monthly charge (GST excl.) |
|---|---|---|---|
| Mail and Web | $22.73 | Up to 5 registered users | $22.73 |

# Part D – Mail and Web Protection / Mail and Web Control

| Service package | Set up fee (once off) (GST excl.) | Maximum number of registered users | Monthly charge (GST excl.) |
|---|---|---|---|
| Protection | | Up to 10 registered users | $40.91 |
| | | Up to 20 registered users | $72.73 |
| | | Up to 50 registered users | $159.09 |
| | | Greater than 50 registered users | $2.733 per registered user |
| Mail and Web Control | $22.73 | Up to 5 registered users | $27.27 |
| | | Up to 10 registered users | $50.00 |
| | | Up to 20 registered users | $90.91 |
| | | Up to 50 registered users | $204.55 |
| | | Greater than 50 registered users | $3.644 for eachper registered user |

**Additional domain name aliasing**

5.2 We will charge you a once off fee of $80 for each additional domain you require to be aliased to either the Protection or Control service packages (or both).

**Registered usage**

5.3 We will commence charging you the fees and charges applicable to the Protection and the Control service packages from the date that the service is made available to you. The charges for the Protection or Control service package will relate to the number of users being scanned by the relevant service (the "**registered usage**").

5.4 The initial charge will relate to the registered usage notified to us by you upon ordering a Protection or Control service package.

5.5 If you obtain both the Protection and Control service packages, you must specify the same registered usage for both service packages. If you obtain both service packages and

specify different registered usage figures for each service package, we will charge you the monthly charge for both service packages based on the higher registered usage figure you specify.

**Payments and variations**

5.6 The Protection and Control service packages will be charged in advance on a single monthly invoice. All charges are payable within 30 days of the date of invoice.

**Changes to the registered usage**

5.7 You must notify us as soon as possible if at any time the number of users being scanned exceeds the registered usage.

5.8 You may change the registered usage by notice to us. We will charge you the monthly charge applicable to the varied registered usage rounded up to the applicable maximum number of registered users set out in the fees and charges table.

5.9 We may also monitor your actual usage of the Protection or Control services and if we determine that the actual number of users being scanned exceeds the registered usage, then we will notify you and provide to you a revised total of the number users being scanned.

**Additional invoicing due to increase in registered usage**

5.10 We may issue additional invoices and adjust subsequent invoices to cover charges for the increase in registered usage on a retrospective basis.

## 6 Email anti virus service

**What is the email anti virus service?**

6.1 The email anti virus service is an Internet level email virus scanning service using commercially available anti virus software.

**Configuration details**

6.2 You are responsible for making the relevant configuration changes that we will tell you at the time you apply for the email anti virus service.

**Scanning attachments, macros or executables**

6.3 We will try to scan all of the email or its attachments, macros or executables that are

directed through the email anti virus service for known viruses. We may not be able to scan certain content, for example password protected or encrypted content.

**What happens if we detect a potential virus?**

6.4 You may set certain configuration options through the online tool to set how the email virus scanning service will handle emails with a potential virus.

6.5 You can configure the email anti virus service so that when it detects a known virus in an inbound email, then an automatic alert will be sent to the sender, intended recipient or both. If the email anti virus service detects a known virus in an outbound email, the service may notify the sender only and not the intended recipient. A notification may also be sent to your nominated administrator in both cases.

6.6 In the case of a major breakout of a new virus, we will post an alert message on our web site (or through such other communications we reasonably consider appropriate) as soon as practicable.

6.7 Any email infected with a potential virus is stored in a secure environment and will be:

(a) if the potential virus is a mass mailer virus, immediately and automatically deleted; and

(b) for all other viruses, automatically deleted after 30 days.

**Release of a virus infected email**

6.8 By completing our release authorisation form, you can ask us to release an email with a potential virus. We will then release that email either to the first address of the original recipient or to an alternative address which is not a third party. If the original recipient is an email group, then the email will be released to all recipients in that email group.

6.9 We will release a virus infected email within eight business hours of receipt of a duly authorised release request.

**Certain emails will not be released**

6.10 We will not:

(a) release certain emails with viruses that have been identified as particularly infectious or damaging;

(b) return a virus-infected email to the sender; or

(c) forward a virus-infected email to a third party.

## 7 Email anti spam service

**What is the email anti spam service?**

7.1 The email anti spam service is an Internet level email anti spam service which is designed to protect you from spam.

7.2 We will scan your inbound email using a number of different detection methods. If an inbound email is suspected as being spam, then the email anti spam service will automatically take one or more of the actions configured by you.

**Configuration options**

7.3 We will initially enable the email anti spam service for each of your domain names you notify us. You are responsible for setting configuration options for each domain through the online tool to set how the email anti spam service will handle suspected spam.

7.4 You may configure certain options for specifying the actions to be taken should an email be suspected as being spam, including (in increasing severity):

(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 email anti spam service);

(d) delete suspected spam email; and

(e) redirect email to spam quarantine.

**Whitelist detection**

7.5 You may compile and upload a private whitelist. If you select this detection method and an incoming email is received from a whitelisted domain, then it will automatically bypass any other selected spam detection methods.

**Blacklist detection**

7.6 You may compile and upload a private blacklist or use a number of public blacklists. If any of these detection methods are selected and an incoming email is received from a

blacklisted domain, then the email anti spam service will take the action configured by you through the online tool.

**Signaturing detection**

7.7 If the email has not been deleted as a result of previous actions 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 blacklist detection, then your inbound email is scanned using the signaturing system.

7.8 If an email is detected by the signaturing method as being spam, then the email anti spam service will take the action configured by you. This action will supersede any less severe action previously determined by any of the blacklist methods.

**Heuristics detection**

7.9 If an email has not been deleted as a result of previous actions and heuristics detection is selected and the action that would be taken as a result of detecting the email as spam as configured by us is more severe than that already selected as a result of detection by the preceding processes, then your inbound email is scanned using heuristics scanning.

7.10 If an incoming email is heuristically detected as being spam, then the email anti spam service will take the action configured by you. This action will supersede any less severe action previously allocated by any of the preceding methods.

**Spam quarantine description**

7.11 If you configure spam quarantine for a domain, each of your spam quarantine accounts will be set up automatically the first time a suspected spam is identified by the email anti spam service and you will automatically receive an email notification.

7.12 You may access spam quarantine through the online tool.

7.13 The email anti spam service will store the suspected spam up to 14 days after which it will be automatically deleted.

7.14 If spam quarantine is not able to accept an email, then the suspected spam email will be tagged and sent to the recipient.

**Spam quarantine configuration**

7.15 You may configure certain notification options in relation to your spam quarantine account. You may select one of the following notification options:

(a) notifications to be received daily;

(b) notifications to be received at a defined frequency; or

(c) notifications not to be received.

7.16 You may configure the following release options for any email tagged as spam:

(a) delete email;

(b) release email to original recipient address; and

(c) review text of email.

7.17 Through the online tool, you may control other aspects of the email anti spam service, including:

(a) automated or manual notification policy;

(b) setup of summary notifications;

(c) default language settings;

(d) whitelisting requests;

(e) preset alias emails; and

(f) specialised users (for example, a quarantine administrator).

**Reporting**

7.18 We will provide you with reports through the online tool or you can configure the email anti spam service to send you reports by email on a weekly or monthly basis.

**General**

7.19 We emphasize that the configuration of the email anti spam service is entirely in your control and recommend that you have an acceptable computer use policy (or its equivalent) in place.

## 8 Image control service

**What is the image control service?**

8.1 The image control service is an internet level email anti-pornography service which is designed to detect pornographic images contained in image files. You acknowledge that what does and does not constitute a pornographic image is a subjective definition.

8.2 The image control service will scan your inbound and outbound email using image

composition analysis for pornographic images contained in image files attached to an email.

**Configuration**

8.3 We will configure the image control service for each of your domains in accordance with the configuration options you notify us from time to time.

8.4 You can set the level of detection sensitivity to high, medium or low. These settings are particularly subjective, and 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.

8.5 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. We recommend that these options be set in line with your acceptable computer use policy (or its equivalent).

8.6 These configuration options are:

(a) log suspected email;

(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; and

(e) delete suspected email.

8.7 If you choose to redirect or delete email containing a suspected pornographic image, then an automatic alert will be sent to the sender. If the email is inbound to you, then an automatic alert is also sent to the intended recipient.

**Reports**

8.8 We will provide you with reports through the online tool or you can configure the image control service to send you reports by email on a weekly or monthly basis.

**General**

8.9 You acknowledge that the image control service may not be able to scan:

(a) attachments with certain content (for example, password protected or encrypted content); and

(b) pornographic images embedded in documents or file types other than image file

types.

8.10 If you release or request the release of a virus infected email, then the released email will not be scanned by the image control service prior to release.

## 9 Content control service

**What is the content control service?**

9.1 The content control service is a service designed to enable you to configure your own rule based filtering strategy in line with your acceptable use policy (or its equivalent) in relation to email.

9.2 The content control service allows you to build a collection of rules upon which incoming and outgoing email is filtered.

9.3 A rule is an instruction you set up to identify a particular format of message/attachment or content with a particular course of action to be taken in relation to the email.

**Configuration**

9.4 You are responsible for determining the configuration options for the content control service for each domain according to your needs and notify those configuration options to us through the online tool.

9.5 You may configure rules on a 'per domain', 'per group' or 'individual' basis.

9.6 If you change a rule, then that change will become effective within 24 hours of being made.

9.7 You may configure the options setting out the action to be taken upon detecting a suspected email. These configuration options may be set independently for inbound and outbound email. We recommend that these options be set in line with your acceptable use policy (or its equivalent).

9.8 These configuration 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; and

(f) log only to statistics.

**Content Control Support**

9.9 As part of the content control service, we will provide you with the following basic support features:

(a) a training session (via WebEx or by phone) to walk through the content control interface including a service description and Q&A session; and

(b) a user guide.

**Reporting**

9.10 You may request reports on the results of your rules in the form of daily, weekly, monthly and annual summaries organised by both rule and by user.

9.11 If you request, then we may generate reports and provide those reports to you through email containing service activity logs on a weekly or monthly basis.

**General**

9.12 You accept and agree that we (or our external suppliers) may compile and publish default word lists using words obtained from your custom word lists.

9.13 You acknowledge that if the content control service is used in conjunction with the quarantine action of the email anti spam service, then this may result in suspected spam being quarantined before it has been filtered by the content control service.

9.14 The content control service may not be able to scan attachments with certain content (for example, password protected or encrypted content).

9.15 If you release or request the release of a virus infected email, then the released email will not be scanned by the content control service prior to release.

## 10 Web anti spyware and anti virus service

**What is the web anti spyware and anti virus service?**

10.1 The web anti spyware and anti virus service is designed to scan a request for web pages and attachments that have been electronically routed through the service for known viruses.

10.2 Your external HTTP and FTP-over-HTTP requests including all attachments, macros or executables are directed through the web anti spyware and anti virus service. Other content routed though HTTP (for example streaming media) can also be passed through the service but will not be scanned.

**Configuration**

10.3 The configuration settings required to direct this external traffic via the web anti spyware and anti virus service are made and maintained by you and are dependent on your technical infrastructure.

10.4 You must ensure that internal HTTP/FTP-over-HTTP traffic (for example, to the corporate intranet) is not directed via the web anti spyware and anti virus service.

10.5 Where you have an Internet service that mandates a direct connection rather than via a proxy, you are responsible for making the necessary changes to your own infrastructure to facilitate this.

10.6 Access to the web anti spyware and anti virus service is restricted via "Scanning IP" which are the IP address(es) from which your web traffic originates. The Scanning IPs are also used to identify the customer and dynamically select customer-specific settings.

10.7 The web anti spyware and anti virus service 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 or encrypted content).

10.8 Attachments specifically identified as not capable of being scanned will be blocked by the web anti spyware and anti virus service.

10.9 Streamed and encrypted traffic (that is, Streaming Media and/or HTTPS/SSL) cannot be scanned and will pass through the web anti spyware and anti virus service unscanned.

**Alerts**

10.10 If your web page or attachments are found by the web anti spyware and anti virus service to contain a virus, spyware or adware, or if the web page or attachment cannot be scanned, then access to that web page or attachment is denied. The web anti spyware and anti virus service will display an automatic alert web page that you specify to the relevant user.

10.11 In certain 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.

## 11 Web URL filtering service

### What is the web URL filtering service?

11.1 The web URL filtering service is designed to filter out certain URLs or access to certain web pages based on an access restriction policy that you determine.

11.2 You must direct your external HTTP and FTP-over-HTTP requests, including all attachments, macros or executables through the web URL filtering service. After you have made the relevant configuration changes, your requests for web pages and attachments are electronically routed via the web URL filtering service and digitally examined.

### Configuration

11.3 You must configure your external web traffic through the web URL filtering service and maintain any necessary configurations.

11.4 You are responsible for configuring your systems so that they do not direct your internal HTTP/FTP-over-HTTP traffic (for example, to the corporate intranet) through the web URL filtering service.

11.5 Where you have Internet services that require a direct connection rather than via a proxy, it is your responsibility to make the necessary changes to your own infrastructure to facilitate this.

11.6 Access to the web URL filtering service is restricted via "Scanning IP" which are the IP address(es) from which your web traffic originates. The Scanning IPs are also used to identify you and dynamically select your specific settings.

11.7 You are responsible for configuring the web URL filtering service to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific users or groups.

### Alerts

11.8 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 or will be sent an optional email.

11.9 In certain 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.

## 12 Service levels

### About service levels

12.1 The service levels set out in this section are indicative targets only. We will endeavour to provide Protection and Control services to meet such indicative service levels, but do not promise the provision of continuous or fault free services.

12.2 We will only commence monitoring the performance of a Protection or a Control service against the relevant service level 30 days after the date you commence using that service.

12.3 The relevant service level will not apply to the Protection or Control services:

(a) during the period your system configuration is not compliant with all relevant standards and guidelines as advised by us from time to time;

(b) during each period of planned maintenance;

(c) during each period a Protection or a Control service is not available to you due to an event beyond our reasonable control or your actions or omissions;

(d) during each period a Protection or a Control service has been suspended in accordance with these terms; or

(e) if you are located in Germany.

### Measurement of service levels

12.4 We will endeavour to provide monthly reports to you setting out our performance of the Protection or Control services against the applicable service levels. We are solely responsible for measuring our performance of the Protection and the Control services against the relevant service levels.

### Latency

12.5 The latency service level set out in this section will only apply to the Protection and the Control services which scan or process an email.

12.6 We will measure the round trip time for your emails sent and received through the Protection or the Control service each calendar month. The service level applicable to the average round trip time is set out in the table below.

| Description | Service level |
|---|---|

# Part D – Mail and Web Protection / Mail and Web Control

| Description | Service level |
|---|---|
| Average roundtrip time of your email through the Protection or the Control service | 95% of emails with a roundtrip time of 2 minutes or less. |

12.7 The latency service level set out in this section will not apply in the following circumstances:

(a) for the period there is a virus outbreak where the virus to email ratio is greater than 1:200;

(b) the period you are responsible for a denial of service attach or suffers a denial of service attack from a third party; or

(c) the period there are any configuration issues beyond our control, including in relation to your SMTP server and domain name system configurations (eg mail-loops).

**False positives**

12.8 This false positives service level set out in this section will only apply to the email anti spam service.

12.9 We will endeavour to ensure that the false positive capture rate does not exceed 0.0004% of all your email traffic in any calendar month.

12.10 The following emails will not constitute false positive emails:

(a) emails which do not constitute legitimate business email;

(b) emails containing more than 20 recipients;

(c) emails in which less than 80% of the email content is in native English;

(d) where the sender of the email is on your blacklist;

(e) emails which are sent from a compromised machine;

(f) emails which are sent from a machine which is on a third party block-list; and

(g) emails which have been sent to more than 20 recipients and have at least 80% the same in content.

12.11 If you ask us to investigate suspected false positive emails and:

(a) our investigation determines that the email is not a false positive email; or

(b) you have agreed to pay the charge,

then we may charge you an administration charge of $100.00 per hour for the time we took to investigate that issue.

**False negatives**

12.12 This false negatives service level set out in this section will only apply to the email anti spam service.

12.13 We will endeavour to ensure that the false negative capture rate does not exceed 5% of all your email traffic through the email anti spam service in each calendar month.

12.14 The false negative service level set out in this section will not apply if:

(a) you have not implemented our best practice for configuration; and

(b) the email was not sent to a legitimate address.

12.15 If you ask us to investigate suspected false negative emails and:

(a) our investigation determines that the email is not a false negative; and

(b) you have agreed to pay the charge,

then we may charge you an administration charge of $100.00 per hour for the time we took to investigate that issue.

**Virus infection**

12.16 The virus infection service level set out in this section will only apply to the anti virus service.

12.17 If we detect but do not stop a virus-infected email, then we will endeavour to promptly notify you, and will endeavour to provide sufficient information to enable you to identify and delete the relevant email.

**Web service availability**

12.18 This web service availability service level set out in this section will only apply if you obtain one or more of the web-based Protection or Control services.

12.19 The service level applicable to web service availability is set out in the table below:

| Description | Service level |
|---|---|
| Web service availability | 100% each calendar month |

## 13 Special meanings

13.1 The following words have the following special meanings:

**bulk email** means a group of more than 5000 email messages instigated by you with substantially similar content, sent or received in a single operation or series of operations.

**email** means any message sent or received using the simple mail transfer protocol.

**false negative** means an event where the email anti spam service delivers an email to you that is spam.

**false positive** means an event where the email anti spam service has blocked a legitimate email that is not spam.

**IP** means Internet Protocol.

**latency** means the average round trip time for emails sent each 5 minute period to and from a Protection or Control service.

**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 is also referred to as 'spam relay' or 'public relay'.

**planned maintenance** means maintenance that we or our suppliers have scheduled to perform on the systems we use to provide the Protection and Control service.

**service availability** means the time the Protection or the Control service applicable to the scanning or processing of an email is available to accept a connection on port 25 to accept an incoming SMTP session.

**spam** means unsolicited commercial email.

**URL** means the uniform resource locator.

**user** means a person or mailbox on behalf of which email is being scanned by the relevant Protection or Control service.

**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.

**web service availability** means the time the Protection or Control service is available to successfully accept your outbound web requests from your correctly configured host.