Our Customer Terms
Internet Solutions section
Part D – Internet Protection Services

Contents

Click on the section you're interested in.

1	**About this section**	**4**
	Words with specific meanings	4
	Our Customer Terms	4
	Inconsistencies	4
	When this section applies	4
	No assignment or resupply	4
	We have to approve your requests	4
	We usually work in Business Hours	5
2	**Internet Protection Services**	**5**
	What are the IPS?	5
	Special requirements to obtain IPS	5
	Intellectual property rights in the IPS	5
	Licence to use related software	5
	Location used to provide IPS	5
	Service not issue free	6
	What we can do if there are security threats	6
	Installing and using services as per our instructions	6
	Online portal	6
	Additional reporting	6
	Changes to your IPS	6
	You can access our help desk	6
3	**Internet Protection Web**	**7**
	What is the Internet Protection Web service?	7
	What is the web malware scanning service?	7
	What is the web content control service?	8
	What is the web filtering service?	8
	What is the outbreak intelligence service?	8
	What is the portal reporting service?	8
	What is the collective security intelligence service?	9
	What is the centralised policy management service?	9
	What is the file reputation service?	9
	What is the file sandboxing service?	9
	What is the file retrospection service?	9
	What are the Internet Protection Web service optional features?	9
	What is the HTTPS inspection service?	10
	What is the connector service?	10
	What is the any connect service?	10
	What is the passive identity management service?	10
	What is the cognitive threat analytics (CTA) service?	11
	What is the advanced active directory integration service?	11
	What is the log extraction service?	11
	What is the data retention service?	11
	Configuring your traffic to use Internet Protection Web	11
4	**Internet Protection Mail**	**12**
	What is the Internet Protection Mail service?	12
	What is the anti-virus service?	13
	What is the email content control service?	13

IT'S HOW WE CONNECT

What is the anti-spam service? 14
What is the forged email filter service? 14
What is C-level impersonation filter service? 14
What is the mail system failover service? 14
What is the alerts on system unavailability service? 14
What is the secure portal RBAC service? 15
What is the centralised policy management service? 15
What is the unified portal (basic applications) service? 15
What is the trace application with 3-day replay service? 15
What is the data loss prevention and risk application service? 15
What is the SPF filter (email spoofing) service? 15
What is the DKIM filter (email spoofing) service? 16
What is the typo domain filter service? 16
What is the Office 365 mail security service? 16
What is the email spooling service? 16
What is the URL filtering (basic) service? 16
What is the URL filtering (advanced) service? 16
What is the advanced malware protection (AMP) service? 16
What is the extended trace application (32 days) service? 17
What is the extended trace application (36 months) service? 17
What is the secure portal RBAC (3 roles) service? 17
What is the secure portal RBAC (up to 6 roles) service? 17
What is the image control application service? 17
What are the Internet Protection Mail service optional features? 17
What is the 7-year archive with trace and replay service? 18
What is the log feeds to SIEM service? 18
What is the two factor authentication service? 18
What is the self-release service? 18
What is the custom applications service? 18
What is the encryption service? 18
There are requirements and limitations to the service 18
Email queue lengths 19

5 Internet Protection Web and Mail bundle 19

6 Internet Protection Hybrid 19
What is the Internet Protection Hybrid service? 19
Internet Protection Hybrid equipment 20
What happens when your equipment becomes obsolete? 21

7 Email Security Audit 22
What is the Email Security Audit service? 22

8 What are your obligations? 22

9 What fees and charges apply? 24
How we charge you for your IPS 24
If your registered usage changes, so will your fees 24
Internet Protection Web charges 24
Internet Protection Web Essentials charges 25
Internet Protection Web Premium charges 25
Internet Protection Mail charges 26
Internet Protection Web and Mail charges 27
Internet Protection Hybrid charges 28
Email Security Audit charges 29
What other charges apply? 29

IT'S HOW WE CONNECT

10	**What service levels apply?**	**29**
	Which services have service levels?	29
	How do I claim a rebate?	30
	How we measure service levels	30
	Platform availability service level	30
	Internet Protection Mail performance service level	31
	Internet Protection Mail accuracy service level	31
	Internet Protection Web performance service level	32
	Internet Protection Web – false-positive web filtering rate	33
	Internet Protection Web – false-negative web filtering rate	33
11	**Minimum term and termination**	**34**
	What's the minimum term for the IPS?	34
	Terminating an IPS	34
12	**Special meanings**	**35**

IT'S HOW WE CONNECT

1 About this section

Words with specific meanings

Certain words are used with the specific meanings set out:

(a) on page 35;

(b) in Part A – Telstra Internet Direct section of the Internet Solutions section; and

(c) in the General Terms of Our Customer Terms ("**General Terms**").

Our Customer Terms

1.2 This is Part D - Internet Protection Services of the Internet Solutions section of Our Customer Terms. This part D only applies if you have one or more IPS.

1.3 The General Terms and provisions in other parts of the Internet Solutions section may also apply to your IPS.

1.4 For more detail on how the various sections should be read together, see clause 1 of the General Terms and clause 1 of Part A – General Terms of Internet Solutions.

Inconsistencies

1.5 This section applies to the extent of any inconsistency with the General Terms or other parts of the Internet Solutions section.

1.6 If a provision of this section lets us suspend or terminate your service, that's in addition to our rights to suspend or terminate your service under the General Terms.

When this section applies

1.7 This section applies if you signed up for your IPS on and from 23 March 2017.

No assignment or resupply

1.8 IPS aren't available to Telstra wholesale customers or for resale. You mustn't assign or resupply IPS to a third party.

We have to approve your requests

1.9 In this section, where you can apply, request, ask, choose, are eligible (or any other similar wording) for a service, feature, functionality, or any other item ("**Request**"), we can accept or reject that Request at our choice. For example, we may reject your Request if IPS isn't available in your area, or your equipment isn't compatible with IPS.

We usually work in Business Hours

1.10 Unless otherwise stated, we perform work as part of IPS (including installation, configuration, site audits and feasibility studies) during Business Hours. Additional charges apply outside Business Hours. We can confirm these charges on request.

2 Internet Protection Services

What are the IPS?

2.1 The IPS are a suite of security services for your web and email traffic. You can apply for one of more of the following:

(a) Internet Protection Web;

(b) Internet Protection Mail;

(c) Internet Protection Web and Mail;

(d) Internet Protection Hybrid; and

(e) Email Security Audit,

being the Internet Protection Services ("**IPS**").

Special requirements to obtain IPS

2.2 When you apply for IPS and from time to time, we'll let you know of any restrictions or specific requirements you must meet to obtain and use the IPS. These requirements are above any requirements in this section and you must meet those requirements at all times.

Intellectual property rights in the IPS

2.3 The intellectual property rights in the IPS and any hardware, software or any other component used in connection with the IPS are and will at all times remain our property or that of our licensors or suppliers (as applicable).

Licence to use related software

2.4 We procure the right for you to use software that is part of the IPS or is needed to use the IPS. This is usually on the same terms that our vendor grants such licences.

2.5 You must comply with (and ensure all your end users comply with), all applicable licence terms at all times.

Location used to provide IPS

2.6 Subject to applicable law, we may provide the IPS from any hardware or other installation anywhere in the world at our choice.

2.7 We don't promise that any installation or any part of it is dedicated to your sole use.

IT'S HOW WE CONNECT

Service not issue free

2.8 We don't promise to supply the IPS at all times without any outages, faults or delays. We don't promise we can fix all defects, problems or issues.

What we can do if there are security threats

2.9 If we reasonably think that the provision of an IPS compromises or may compromise the security of the IPS or our network (for example, due to hacking attempts or denial of service attacks), then we may temporarily suspend the service.

2.10 We'll try and tell you if we temporarily suspend your IPS. We'll then try and work with you to with the aim of re-instating the service to you.

Installing and using services as per our instructions

2.11 At all times, you must ensure that the IPS is installed and used as per the installation guidelines which we provide and as per our instructions from time to time.

2.12 The IPS may not work on all systems and set-ups. We'll confirm which ones are compatible around the time you apply for the service.

Online portal

2.13 You can access an online portal to configure, manage or request reports on the IPS.

2.14 Your Internet Protection Web and Internet Protection Mail service will have their own separate online portal.

2.15 We'll try to tell you of emergencies or any maintenance that may materially and detrimentally affect your IPS. We may do this by posting a message on the online portal.

Additional reporting

2.16 We may provide user or group administration and reporting services with the relevant IPS.

Changes to your IPS

2.17 We can change any part of the IPS or the IPS platform without telling you, but only if it doesn't materially and detrimentally affect your IPS.

You can access our help desk

2.18 We'll give you access to a help desk that aims to be available 24 hours a day, 7 days a week.

2.19 We'll give you the help desk's details, including contact details when you request an IPS.

2.20 You must report all faults with your IPS to our help desk and give us details of the fault and all other information we request so we can investigate the fault.

3 Internet Protection Web

What is the Internet Protection Web service?

3.1 The Internet Protection Web service aims to provide security features for your web traffic. You can choose from the "Essentials" or "Premium" package:

INTERNET PROTECTION WEB		
Feature	**Essentials**	**Premium**
Web malware scanning	✓	✓
Web content control (web data loss prevention)	✓	✓
Web filtering	✓	✓
Outbreak intelligence	✓	✓
Portal reporting	✓	✓
Collective security intelligence	✓	✓
Centralised policy management	✓	✓
File reputation (AMP)	x	✓
File sandboxing (AMP)	x	✓
File retrospection (AMP)	x	✓
HTTPS inspection	O	O
Connector	O	O
Any connect	O	O
Passive Identity Management (PIM)	O	O
Cognitive threat analytics	O	O
Advanced active directory integration options	O	O
Log extraction	O	O
Data retention	O	O
KEY: ✓ = Included in the package. X = Not available with the package. O = Optional with the package for an additional charge.		

What is the web malware scanning service?

3.2 The web malware scanning service aims to detect known viruses. It does this by scanning requests for web pages and attachments that have been electronically routed through the Internet Protection Web service.

3.3 The web malware scanning service aims to scan the web page and its attachments. However, this isn't always possible (for example, if they are password protected). Un-scannable documents are usually blocked.

3.4 Encrypted traffic can't be scanned and will pass through the web malware scanning service un-scanned unless you have the HTTPS inspection service enabled.

3.5 If a requested web page or attachment is found to contain malware (or if it is un-scannable), then access to that web page or attachment will be denied and an automatic block alert web page will be shown. Your administrator may also be notified by email.

What is the web content control service?

3.6 The web content control service is a web data loss prevention service that lets you define rules to monitor your outbound web traffic based on HTTP protocols. This service can look for specific files with certain characteristics, keyword analysis, preconfigured IDs (for example, credit card or social security numbers) and DFA-based regular expressions.

3.7 If you've enabled the web filtering service, you may also apply the web content control service to your outbound web traffic.

What is the web filtering service?

3.8 The web filtering service aims to filter out certain URLs or access to certain web pages as per the access restriction policies you create.

3.9 Access restriction policies can be based on categories or types of content (or both). You can deploy your policies at specific times and to specific Internet users or groups. You may also select additional features (for example, "blocked" and "allowed" list functionality). You may configure specific exceptions for web sites that won't be filtered.

3.10 The web filtering service will try and filter the web page and its attachments based on the categories and/or types of content you chose to filter. However, this may not always be possible (for example, if they are password protected).

3.11 If you request a web page or attachment to which an access restriction policy applies, then that access will be denied and an automatic block alert web page will be shown. Your administrator may also be notified by email.

3.12 Unless you enable the HTTPS inspection service, encrypted traffic (for example HTTPS/SSL) can't be filtered and will be passed through the web filtering service unfiltered. If you have the HTTPS inspection service enabled, encrypted traffic will be filtered as per your selected policies.

What is the outbreak intelligence service?

3.13 The outbreak intelligence service aims to detect unknown and unusual behaviours and zero-hour outbreaks through a heuristics-based anti-malware engine.

3.14 It does this by running webpage components in a virtual emulation environment before permitting user access. The service opens up the individual components of a webpage to determine how each component behaves and then aims to block any malware.

What is the portal reporting service?

3.15 You can request that your administrators have access to a variety of predefined reports and for them to create customised dashboards and set notifications.

IT'S HOW WE CONNECT

3.16 All reports are generated and stored in the cloud, so they're delivered quickly. Reports can also be saved and scheduled for automated delivery. These capabilities provide flexibility, offering detail down to the user level, and help enable your administrators to spot potential issues quickly.

What is the collective security intelligence service?

3.17 This service collects information on web threats. It does this via product and service telemetry, public and private feeds and the open source community.

What is the centralised policy management service?

3.18 The centralised policy management service aims to offer centralised visibility and management of security and content control policies in the online portal. These policies can help manage bandwidth consumption and restrict access to social media or inappropriate content (such as gambling or pornography).

What is the file reputation service?

3.19 The file reputation service uses advanced analytics and collective intelligence to try and determine whether a file is clean or malicious. The service can analyse files and block or apply respective policies.

What is the file sandboxing service?

3.20 This service aims to provide a secure environment to execute, analyse, and test malware behaviour (for example, by analysing unknown files to understand true file behaviour).

What is the file retrospection service?

3.21 This service aims to protect against malicious files that pass through perimeter defences but are later deemed a threat. It does this by analysing files that have traversed the security gateway, using real-time updates to stay up to date on changing threat tactics.

3.22 Once a file is identified as a threat, administrators are alerted and shown who on the network may have been infected and when. As a result, the service aims to help you identify and address an attack quickly, before it can spread.

What are the Internet Protection Web service optional features?

3.23 You may also request the following optional services with the Internet Protection Web service (additional fees may apply, which we can confirm on request):

(a) HTTPS inspection;

(b) connector;

(c) any connect;

(d) Passive Identity Management (PIM);

(e) cognitive threat analytics;

(f) advanced active directory integration options;

(g) log extraction; and

(h) data retention.

What is the HTTPS inspection service?

3.24 The HTTPS inspection service lets your administrator set a policy to determine which domains and categories of HTTPS traffic are decrypted and subject to the web malware scanning service and / or the web filtering service.

3.25 Data is encrypted from the web server to the scanning tower in the normal way. However, for domains specified in your administrator's policy, the scanning tower will terminate the SSL-based connection, inspect the data using the web malware scanning service and / or the web filtering service, and then re-encrypt the traffic from the scanning towers to the end user using a different certificate.

What is the connector service?

3.26 The connector service aims to let your users connect to the Internet Protection Web service without a static IP address by using an authentication key.

3.27 Your administrators can create, revoke, activate and deactivate authentication keys for the connector service per group or per user.

What is the any connect service?

3.28 The any connect service lets your users connect to the Internet Protection Web service from a remote location outside of your internal network.

3.29 You must request the any connect service for at least 25 users, in increments of:

(a) 5 users between 25 and 100 users (for example, 25, 30, 35, 40 etc); and

(b) 25 users for more than 100 users (for example, 125, 150, 175 etc).

What is the passive identity management service?

3.30 The passive identity management ("**PIM**") service aims to let you:

(a) increase control over your users' access to certain Internet web content, based on the user privileges you've assigned within your domain; and

(b) review and report on your users' Internet web usage at an individual user level.

3.31 We'll give you the PIM software and support, installation guidelines, design support, and release notes detailing which operational systems and browsers are supported.

3.32 You're solely responsible installing and using the PIM software as per clause 2.11.

3.33 Additional fees may apply for the PIM service, depending on your systems and set up. We can confirm these fees on request.

What is the cognitive threat analytics (CTA) service?

3.34 The CTA service is a service that:

(a) uses machine learning and statistical network modelling;

(b) creates a baseline of the traffic in your network and looks for anomalies;

(c) analyses user and device behaviour and web traffic;

(d) aims to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure;

(e) aims to reduce the discovery time of threats operating inside the network; and

(f) aims to address gaps in perimeter-based defences by identifying symptoms of malware infection or data breach via behavioural analysis and anomaly detection.

3.35 You must apply for the CTA service for at least 1000 users. We'll confirm applicable fees on request.

What is the advanced active directory integration service?

3.36 Advanced active directory integration allows authentication / identification by integration with active directories for policy control and reporting down to user group level.

What is the log extraction service?

3.37 This service aims to let you extract web usage data for secure analysis. Formatted in W3C text format, data can be used to analyse security information and event management.

What is the data retention service?

3.38 Data retention aims to retain:

(a) blocked web requests (policy or malware blocks) for one year; and

(b) allowed data for 45 days.

Configuring your traffic to use Internet Protection Web

3.39 To use the Internet Protection Web service, you must ensure your external traffic is directed through the Internet Protection Web service at all times.

3.40 We don't promise that the Internet Protection Web service will function for web traffic that you haven't routed in the way we recommend from time to time.

IT'S HOW WE CONNECT

3.41 You're responsible for configuring your systems to direct external traffic through the Internet Protection Web service.

3.42 You must ensure that your internal traffic (for example traffic to your corporate intranet) isn't directed through the Internet Protection Web service.

4 Internet Protection Mail

What is the Internet Protection Mail service?

4.1 The Internet Protection Mail service aims to provide security features for your email traffic. You can choose from the "Essentials", "Enhanced" or "Premium" package:

INTERNET PROTECTION MAIL			
Feature	**Essentials**	**Enhanced**	**Premium**
Anti-virus	✓	✓	✓
Email content control	✓	✓	✓
Anti-spam	✓	✓	✓
Forged email filter	✓	✓	✓
C-level impersonation filter	✓	✓	✓
Mail system failover	✓	✓	✓
Alerts on system unavailability	✓	✓	✓
Secure portal RBAC	✓	✓	✓
Centralised policy management	✓	✓	✓
Unified portal apps (basic apps)	✓	✓	✓
Trace app with 3 day replay	✓	✓	✓
Data loss prevention & risk app	✓	✓	✓
SPF filter (email spoofing)	✓	✓	✓
DKIM filter (email spoofing)	✓	✓	✓
Typo domain filter	✓	✓	✓
Office 365 mail security	✓	✓	✓
Email spooling	✓	✓	✓
URL filtering (basic)	✓	✓	✓
URL filtering (advanced)	x	✓	✓
Advanced Malware Protection (AMP)	x	✓	✓
Extended trace application (32 days)	x	✓	✓
Extended trace application (up to 36 months)	x	x	✓
Secure portal RBAC (up to 3 roles)	x	✓	✓
Secure portal RBAC (up to 6 roles)	x	x	✓
Image control application	x	x	✓
7-year archive with trace and replay	O	O	O
Log feeds to SIEM or other	O	O	O

Two factor authentication	O	O	O
Self-release	O	O	O
Custom applications	O	O	O
Encryption	O	O	O

KEY:
✓ = Included in the package.
X = Not available with the package.
O = Optional with the package for an additional charge.

What is the anti-virus service?

4.2 The anti-virus service uses anti-virus engines to scan incoming SMTP email messages (and scannable attachments) and aims (but doesn't guarantee) to block known viruses.

4.3 Where the anti-virus service detects a virus, it will try to delete or repair the email message (including any attachments).

What is the email content control service?

4.4 This service offers inbound and outbound email classifiers and policy filters. These are configurable, viewable & reportable via the online portal. They're based on classification algorithms described below with some employing machine learning technologies.

4.5 The email classifiers include:

(a) **invoice** – classifies emails with invoices in the message body;

(b) **social networking** – classifies emails from domains owned by compatible social network platforms; and

(c) **recruitment** – classifies emails from detected recruiters or recruitment agencies.

4.6 The policy filters include:

(a) address only;

(b) email size;

(c) attachment type;

(d) profanity;

(e) PCI (or payment card industry security standard);

(f) custom keywords; and

(g) inbound marketing – the inbound marketing filter scans and tags (in the subject header) all mail identified as "marketing" communications. Policies can be configured to block, alert or quarantine this mail.

What is the anti-spam service?

4.7 The anti-spam service uses software to scan incoming SMTP email messages and attachments and aims (but doesn't guarantee) to reject known spam.

4.8 Where the anti-spam service determines that an email message is spam, it will delete the email message (including any attachments). We don't have to tell you when this happens.

What is the forged email filter service?

4.9 The forged email filter service aims to:

(a) identify various types of email forge attempt; and

(b) protect against phishing emails that are diagnosed as being sent from a trusted source (e.g. Internal staff member's email or application execution, financial institution or known association).

What is C-level impersonation filter service?

4.10 The C-level impersonation filter service:

(a) aims to protects your employees in specific roles, (such as finance and accounts payable), against targeted impersonation email attack types variously known as CEO impersonation fraud, "whaling", "bogus boss" email scams or business email compromise; and

(b) uses "fuzzy-matching" algorithms to analyse inbound emails with the aim of detecting attempts to impersonate a senior officer.

What is the mail system failover service?

4.11 The mail system failover service aims to automatically switch to a secondary mail server if the primary mail server is unreachable and meets a specified time condition. This helps ensure continuity of your mail system.

4.12 Failing back to the primary mail server is a manual process, which you can do via the online portal.

4.13 The mail server failover is handled by the online portal. You can add a secondary mail server address via the online portal.

4.14 If your primary mail server is offline, you can set up SMS or email alerts to be sent out or you can request a call from us during Business Hours.

What is the alerts on system unavailability service?

4.15 The alerts on system unavailability service aims to:

(a) monitor the performance of an Internet Protection Mail service; and

(b) send alerts to specified users when it detects your mail server is down.

What is the secure portal RBAC service?

4.16 The secure portal RBAC service aims to provide your authorised IT administrator with access to the online portal.

What is the centralised policy management service?

4.17 The centralised policy management service aims to offer centralised visibility and management of security and content control policies in the online portal. These policies can help manage bandwidth consumption and restrict access to social media or inappropriate content (such as gambling or pornography).

What is the unified portal (basic applications) service?

4.18 The unified portal (basic applications) service aims to provide a unified security portal with applications for visibility, policy controls and reporting.

What is the trace application with 3-day replay service?

4.19 The trace application with 3-day replay service aims to offer advanced search and retrieval of inbound and outbound emails for a retrospective time period of up to 3 days.

What is the data loss prevention and risk application service?

4.20 The data loss prevention and risk application service aims to provide data loss prevention capabilities on your outbound email. It looks for specific files with certain characteristics, keyword analysis, pre-configured IDs (for example, credit card or social security numbers) and certain regular expressions, using the below filters:

(a) **credit card (Payment Card Industry – PCI) filter:** This matches the patterns of known credit cards (using a complex regular expression) and applies the "Luhn Check" (used by many e-commerce sites) for validation of the credit card number.

(b) **custom keywords filter:** This accepts words or phrases to match in the email. The following parts of the email are joined together before the match is applied:

(i) subject line text;

(ii) body text; and

(iii) body html (after conversion to text).

What is the SPF filter (email spoofing) service?

4.21 The SPF filter (email spoofing) service uses the industry standard "Sender Policy Framework" email validation system to try to detect and block forged or spoofed emails.

IT'S HOW WE CONNECT

What is the DKIM filter (email spoofing) service?

4.22 This service uses the industry standard "Domain Keys Identified Mail" ("**DKIM**") digital signature based email sender domain authentication and integrity system, to try to detect and block illegitimate forged or spoofed inbound emails.

What is the typo domain filter service?

4.23 The typo domain filter service uses algorithms to analyse inbound emails to try to detect and label or block those that appear to come from a well-known domain name but actually originate from a homograph ("lookalike") domain name (e.g. By using special extended characters that disguises their true origin).

What is the Office 365 mail security service?

4.24 The Office 365 mail security service aims to deliver an additional layer of advanced inbound and outbound email security for Office 365 Exchange Online (SaaS) customers.

4.25 Your outbound emails sent from the Office 365 cloud (from email configured domains configured through the IPS), are verified using DKIM authentication before proceeding for processing via the IPS.

What is the email spooling service?

4.26 This is a disaster recovery service that supports spooling of inbound emails that can't be delivered due to your mail server being unreachable or unavailable for up to 5 days.

What is the URL filtering (basic) service?

4.27 This service aims to detect and quarantine emails with malicious URLs. This can reduce exposure to cyber threats (e.g. Phishing attacks or links to malware infected web sites).

4.28 All emails containing any URLs detected as malicious are automatically quarantined. These emails can be viewed offline by your IT administrator.

What is the URL filtering (advanced) service?

4.29 This service lets you configure more powerful security policies and rules (with a range of match actions), for emails containing malicious, suspect, clean or unknown URLs.

4.30 Advanced reporting on attempted URL security breaches is accessed via the online portal.

What is the advanced malware protection (AMP) service?

4.31 The AMP service aims to deliver protection from advanced persistent threats via email.

4.32 Using file reputation, the AMP service captures a fingerprint of each file as it traverses the gateway and sends it to a cloud-based intelligence network for a reputation verdict. Advanced sandboxing technology can also be used to detect malware, allowing security administrators to glean precise details about a file's behaviour and threat level.

4.33 Using continuous analysis of files, the AMP service looks for malicious files that have passed through the gateway and were subsequently deemed a threat. The AMP service then sends a retrospective alert that gives you visibility into who on the network may have been affected and when.

What is the extended trace application (32 days) service?

4.34 This service can extend the time frame for you to search and replay emails. This time frame is extended for the length of your subscription (up to a maximum of 32 days).

What is the extended trace application (36 months) service?

4.35 This service can extend the time frame for you to search and replay emails. This time frame is extended for the length of your subscription (up to a maximum of 36 months).

What is the secure portal RBAC (3 roles) service?

4.36 This service aims to provide access for up to 3 of your personnel to the online portal. Access can vary between each person to ensure only those who require policy control or visibility to certain reports / applications are given this access.

What is the secure portal RBAC (up to 6 roles) service?

4.37 This service is similar to the above service except it aims to provide access for up to 6 of your personnel to the online portal.

What is the image control application service?

4.38 This service aims to enforce your policies on non-business and offensive images being sent / received from your mailboxes. It aims to identify the following attachments:

(a) common non-business media;

(b) offensive images and videos;

(c) corporate logos; and

(d) smileys and backgrounds.

What are the Internet Protection Mail service optional features?

4.39 You may also request the following optional services with the Internet Protection Mail service (additional fees may apply, which we can confirm on request):

(a) 7-year archive with trace and replay;

(b) log feeds to SIEM (security incident event management) or other;

(c) two factor authentication;

(d) self-release;

IT'S HOW WE CONNECT

(e) custom applications; and

(f) encryption.

What is the 7-year archive with trace and replay service?

4.40 This service aims to extend the time frame for you to search and replay emails. This time frame is extended for the length of your subscription (up to a maximum of 7 years).

What is the log feeds to SIEM service?

4.41 This service aims to let you have log feeds from your email solution to your SIEM solution. It offers you greater consolidation of your security events.

What is the two factor authentication service?

4.42 This service aims to offer two factor authentication access to the online portal. You use it if you want more secure access to the online portal from multiple compatible devices.

What is the self-release service?

4.43 This service lets you self-release emails that you recognise as a policy exception. It can be applied to multiple filters in the online portal so it can notify you of potential policy breaches.

4.44 You can customise the notification sent to you to reflect your brand and organisation policies.

What is the custom applications service?

4.45 We can help develop customised apps on request if you need particular capabilities in reporting, policy setting and security.

What is the encryption service?

4.46 We offer a range of mail encryption options, which we can discuss with you on request.

There are requirements and limitations to the service

4.47 The Internet Protection Mail service won't scan attachments if the file can't be read or opened (e.g. Zip files or encrypted files where the file can't be read without using a decryption device).

4.48 You must have a registered domain name to use the Internet Protection Mail service.

4.49 You must appropriately configure your domain name system to use the Internet Protection Mail service. On request, we can provide technical information on how to do this.

4.50 The service assurance and network availability targets which apply to the Telstra Internet Direct service don't apply to the Internet Protection Mail service.

IT'S HOW WE CONNECT

4.51 We don't promise:

(a) to detect or block all spam, viruses, malware or other harmful programming;

(b) that we won't incorrectly identify some legitimate email messages as spam;

(c) that the Internet Protection Mail service will function for email messages which you haven't routed in the way we tell you to; or

(d) that the Internet Protection Mail service or platform will be free from intrusions, viruses, Trojan horses, worms, time bombs, cancelbots or other similar harmful programming routines.

Email queue lengths

4.52 If we detect a rising email queue for your domain, we may test your receiving mail server's ability to receive email and may tell you if this test fails.

4.53 If we can't deliver email to you, then we may try to store your inbound email for up to three days. After this, your emails and web traffic will be deleted from our systems.

5 Internet Protection Web and Mail bundle

5.1 The Internet Protection Web and Mail bundle is made up of an:

(a) Internet Protection Web service – Essentials package; and

(b) Internet Protection Mail service – Essentials package.

5.2 The applicable terms for the Internet Protection Web and Internet Protection Mail services apply to your Internet Protection Web and Mail bundle.

5.3 You can only terminate your Internet Protection Web and Mail bundle together. You can't terminate the individual services or components that make up that bundle.

6 Internet Protection Hybrid

What is the Internet Protection Hybrid service?

6.1 The Internet Protection Hybrid service aims to provide security for your web traffic. It includes the following equipment and equipment related services:

(a) two web gateways (equipment), including support;

(b) equipment configuration after you connect the equipment to your network; and

(c) equipment monitoring (if you give us or our suppliers access to your equipment).

6.2 The Internet Protection Hybrid service's features include the following:

(a) acceptable use policy controls;

(b) reputation filtering;

(c) malware filtering;

(d) data security; and

(e) application visibility and control.

Internet Protection Hybrid equipment

6.3 We or our suppliers own the equipment we rent to you as part of your Internet Protection Hybrid service. Title to the equipment doesn't pass to you at any time. Risk in the equipment transfers to you on delivery.

6.4 If you cancel an equipment order after we've ordered it from our supplier, on our request, you must promptly pay us for that equipment. This is on top of any of our other rights.

6.5 You must take reasonable care of the equipment and pay for any equipment damage that occurs after it's delivered to you.

6.6 If the equipment is destroyed, lost or stolen at any time, you must at our request, promptly pay us an additional fee to replace the equipment.

6.7 You mustn't modify the equipment (and you must ensure it isn't modified) without our prior written consent, but if that happens:

(a) and the equipment's condition or operation is impaired (or the equipment is diminished in use or value), then we may charge you an additional repair fee, which you must promptly pay on our request;

(b) you must ensure any part replaced during the modification is of equal or better quality than the removed or original part; and

(c) any part of the equipment that's replaced or modified becomes part of the equipment (and is our property).

6.8 At all times and at your cost, you must at all times ensure the equipment (including any replacement equipment we provide) is used solely in:

(a) connection with your Internet Hybrid Protection service at your nominated sites;

(b) a manner contemplated by the manufacturer and as per the manufacturer's manuals and recommendations from time to time;

(c) compliance with all relevant laws;

(d) accordance with our reasonable directions from time to time; and

(e) a suitable environment for the correct operation of the equipment.

6.9 At all times and at your cost, you must at all times:

(a) ensure the availability of necessary auxiliary services for the correct operation of the equipment;

(b) protect the equipment from electrostatic interference and power surges;

(c) ensure the equipment is kept in good order and repair (if you don't, you must on our request, reimburse us for the cost of restoring the equipment); and

(d) allow us (or our agents) to inspect the equipment on reasonable notice.

6.10 You mustn't:

(a) attempt to sell, dispose of or encumber the equipment in any way; or

(b) alter any identifying markings on the equipment.

6.11 If your Internet Protection Hybrid service is cancelled or terminated for any reason, then you must at your cost:

(a) within 14 days of cancellation or termination, deliver the equipment back to us in good working order and condition (reasonable wear and tear excepted) to such place in Australia as we may reasonably direct; and

(b) if applicable, immediately pay us any applicable early termination fees or costs associated with restoring the equipment.

6.12 If you don't deliver the equipment as required under clause 6.11(a), then:

(a) we (or our agent), may enter any premises we believe the equipment may be located to recover it; and

(b) you must promptly pay us any expenses we (or our agent) reasonably incurs in recovering or attempting to recover the equipment.

What happens when your equipment becomes obsolete?

6.13 Over time, we may no longer be able support your equipment ("**Obsolete Equipment**"). We'll tell you if this happens and may recommend (at your cost):

(a) replacement equipment for you; and

(b) a timeframe to implement that replacement equipment.

6.14 If you don't implement our recommendation at your own cost:

(a) we don't guarantee the quality, performance or functioning of any Obsolete Equipment or any IPS that uses or incorporates Obsolete Equipment;

(b) you must promptly pay us to manage or fix any issue caused by any Obsolete Equipment and this is at our then standard time and material rates, which we can confirm on request; or

(c) we may terminate any of your IPS that uses Obsolete Equipment by telling you at least 30 days in advance.

7 Email Security Audit

What is the Email Security Audit service?

7.1 The email security audit service aims to analyse data entering and leaving your network in a 30 day period. On your request, we may agree to extend this in increments of 30 days (60 days, 90 days etc).

7.2 You can request to have the email security audit service undertaken on:

(a) inbound traffic only;

(b) outbound traffic only;

(c) inbound and outbound traffic; or

(d) inbound, outbound and internal traffic.

7.3 During the audit period, the email security audit service aims (but doesn't guarantee), to identify information about your email traffic such as:

(a) the volume of inbound and outbound email;

(b) the volume of email blocked as spam;

(c) details of the email traffic such as attachments, HTML / text and multimedia files;

(d) high usage users; and

(e) potential data loss.

7.4 We can only provide the email security audit service if we have first confirmed that your system is compatible.

7.5 Following completion of the email security audit, we'll give you a report of the results.

8 What are your obligations?

8.1 So we can provide the IPS to you, you must at your cost provide us with:

(a) all complete and accurate relevant information (including technical data, consents and all other information); and

(b) cooperation and assistance,

we may reasonably request from time to time.

8.2 At all times and at your cost, you must:

(a) use the IPS for legitimate business purposes only;

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

(c) promptly comply with our reasonable directions from time to time about the IPS;

(d) not re-sell, sub-lease, sub-rent or sub-license the IPS to any other person, and must not allow any other person to use the IPS without our prior written consent;

(e) not use the IPS in a way that may adversely affect the efficiency, security or use by other people of the IPS.

(f) ensure you inform (for example via a banner message on emails or in your IT policy) those who use any communications system covered by the IPS, that communications transmitted through that system may be intercepted, and indicate the purposes of such interception;

(g) not falsify, forge or otherwise tamper with any portion of the header or tracking data of any SMTP email message;

(h) not use any data obtained via the IPS for any unlawful purpose; and

(i) use the IPS 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) originate, send or relay spam or intentionally launch viruses.

8.3 If you breach clause 8.2(i), we may immediately suspend all or part of your IPS until you rectify the issue to our satisfaction.

8.4 You must at all times and at your own cost:

(a) provide an appropriate person to advise on requirements, access, security procedures and any other matter within your knowledge or control in connection with the IPS;

(b) obtain and keep appropriate equipment, software, telecommunication services, Internet access and other services or resources ("**Facilities**") needed to use the IPS; and

(c) on reasonable notice, let us (or our representative) check that your Facilities have been properly configured and operate correctly with the IPS.

9 What fees and charges apply?

How we charge you for your IPS

9.1 We'll charge you for your IPS in advance on a single monthly invoice.

9.2 We'll charge you for the total number of:

(a) mail boxes, which your IPS will scan;

(b) users, which your Internet Protection Web service or Internet Protection Hybrid service will scan; and

(c) users whose email your Email Security Audit service will scan.

9.3 We'll start charging you from the date we tell you that configuration of your IPS is done.

9.4 All prices in this section are GST exclusive unless otherwise stated.

If your registered usage changes, so will your fees

9.5 You must tell us as soon as possible if at any time, the number of users or mailboxes being scanned exceeds the registered usage.

9.6 You may request to change the registered usage. If we agree to your request:

(a) the monthly charge applicable to the varied registered usage will apply; and

(b) we'll round up to the applicable maximum number of registered users or mailboxes, as set out in the fees and charges table in this section.

9.7 You can't reduce the registered usage of your IPS before the end of your minimum term.

9.8 We may monitor your usage of the IPS. If we think you're exceeding the registered usage, we'll give you a revised total of the number of users or mailboxes being scanned. You must pay us accordingly for this revised total.

9.9 We may issue additional invoices and adjust subsequent invoices to cover charges for the increase in registered usage on a retrospective basis and you must pay these invoices.

Internet Protection Web charges

9.10 If you acquire the Internet Protection Web service only, you must pay us the below:

(a) once off connection charge; and

(b) monthly service charge.

9.11 The monthly service charges in the below tables are subject to your peak bandwidth per user (the higher of inbound and outbound, measured on a 95th percentile basis) not exceeding an average of 5kbps in any calendar month. If this level is exceeded in two or more calendar months in any consecutive 12 month period, we may increase the charges by telling you.

9.12 If you're acquiring the any connect service, an additional charge per end user per month applies to the monthly service charges. We can confirm this charge on request.

Internet Protection Web Essentials charges

INTERNET PROTECTION WEB ESSENTIALS – CONNECTION CHARGE (ONCE OFF)			
No. of users	**Connection type**		
	PIM script based	**Appliance based**	**Connector based**
100 or less	$2,016	$2,016	$8,000
101 to 250	$2,339	$2,339	$8,400
251 to 300	$2,713	$2,713	$8,820
301 to 400	$3,147	$3,147	$9,261
401 to 500	$3,650	$3,650	$9,724
501 to 750	$4,234	$4,234	$10,210
751 to 1000	$4,912	$4,912	$10,721
1001 to 2000	$5,698	$5,698	$11,257
2001 or more	POA	POA	POA

INTERNET PROTECTION WEB ESSENTIALS – SERVICE CHARGE (MONTHLY)			
No. of users	**12 month term**	**24 month term**	**36 month term**
100 or less	$5.78	$5.53	$5.20
101 to 250	$5.15	$4.88	$4.62
251 to 300	$3.87	$3.63	$3.45
301 to 400	$3.87	$3.63	$3.45
401 to 500	$3.87	$3.63	$3.45
501 to 750	$3.25	$3.03	$2.85
751 to 1000	$3.25	$3.03	$2.85
1001 to 2000	$2.92	$2.77	$2.58
2001 or more	POA	POA	POA

Internet Protection Web Premium charges

INTERNET PROTECTION WEB PREMIUM – CONNECTION CHARGE (ONCE OFF)			
No. of users	**Connection type**		
	PIM script based	**Appliance based**	**Connector based**
100 or less	$2,900	$2,900	$9,200

101 to 250	$3,190	$3,190	$9,660
251 to 300	$3,509	$3,509	$10,143
301 to 400	$3,860	$3,860	$10,650
401 to 500	$4,246	$4,246	$11,183
501 to 750	$4,670	$4,670	$11,742
751 to 1000	$5,238	$5,238	$12,329
1001 to 2000	$5,440	$5,440	$12,827
2001 or more	POA	POA	POA

INTERNET PROTECTION WEB PREMIUM – SERVICE CHARGE (MONTHLY)			
No. of users	**12 month term**	**24 month term**	**36 month term**
100 or less	$8.87	$8.34	$8.00
101 to 250	$8.87	$8.34	$8.00
251 to 300	$6.93	$6.46	$6.10
301 to 400	$6.93	$6.46	$6.10
401 to 500	$6.93	$6.46	$6.10
501 to 750	$5.92	$5.54	$5.09
751 to 1000	$5.92	$5.54	$5.09
1001 to 2000	$5.53	$5.24	$4.46
2001 or more	POA	POA	POA

Internet Protection Mail charges

9.13 If you acquire the Internet Protection Mail service only, you must pay us the below:

(a) once off connection charge; and

(b) monthly service charge.

INTERNET PROTECTION MAIL – CONNECTION CHARGE (ONCE OFF)			
No. of mail boxes	**Essentials**	**Enhanced**	**Premium**
100 or less	$1,820	$7,421	$7,953
101 to 250	$2,002	$7,570	$8,167
251 to 300	$2,202	$7,718	$8,926
301 to 400	$2,422	$7,867	$9,562
401 to 500	$2,665	$8,015	$10,208
501 to 750	$2,931	$8,164	$11,289
751 to 1000	$3,224	$8,312	$12,807
1001 to 2000	$3,547	$8,460	$16,480
2001 or more	POA	POA	POA

INTERNET PROTECTION MAIL ESSENTIALS – SERVICE CHARGE (MONTHLY)			
No. of mail boxes	**12 month term**	**24 month term**	**36 month term**
100 or less	$4.92	$4.89	$4.58
101 to 250	$4.32	$4.34	$4.09
251 to 300	$3.26	$3.22	$3.03
301 to 400	$3.26	$3.22	$3.03
401 to 500	$3.26	$3.22	$3.03
501 to 750	$2.72	$2.66	$2.60
751 to 1000	$2.72	$2.66	$2.60
1001 to 2000	$2.60	$2.58	$2.57
2001 or more	POA	POA	POA

INTERNET PROTECTION MAIL ENHANCED – SERVICE CHARGE (MONTHLY)			
No. of mail boxes	**12 month term**	**24 month term**	**36 month term**
100 or less	$7.97	$7.66	$7.52
101 to 250	$7.75	$7.52	$7.38
251 to 300	$7.62	$7.38	$7.29
301 to 400	$7.48	$7.29	$7.20
401 to 500	$7.34	$7.20	$7.11
501 to 750	$7.25	$7.06	$7.02
751 to 1000	$7.06	$6.92	$6.88
1001 to 2000	$6.84	$6.80	$6.75
2001 or more	POA	POA	POA

INTERNET PROTECTION MAIL PREMIUM – SERVICE CHARGE (MONTHLY)			
No. of mail boxes	**12 month term**	**24 month term**	**36 month term**
100 or less	$9.27	$8.90	$8.73
101 to 250	$9.00	$8.73	$8.57
251 to 300	$8.84	$8.57	$8.47
301 to 400	$8.69	$8.47	$8.37
401 to 500	$8.53	$8.37	$8.26
501 to 750	$8.42	$8.20	$8.16
751 to 1000	$8.20	$8.04	$8.00
1001 to 2000	$7.94	$7.89	$7.83
2001 or more	POA	POA	POA

Internet Protection Web and Mail charges

9.14 If you acquire the Internet Protection Web and Mail service, you must pay us the below:

IT'S HOW WE CONNECT

(a) once off connection charge; and

(b) monthly service charge.

9.15 The monthly service charges in the below tables are subject to your peak bandwidth per user (the higher of inbound and outbound, measured on a 95th percentile basis) not exceeding an average of 5kbps in any calendar month. If this level is exceeded in two or more calendar months in any consecutive 12 month period, we may increase the charges by telling you.

9.16 If you're acquiring the any connect service, an additional charge per end user per month applies to the monthly service charges below. We can confirm this charge on request.

INTERNET PROTECTION WEB AND MAIL CHARGES				
No. of users	**Connection charge (once off)**	**Service charge (monthly)**		
		12 month term	**24 month term**	**36 month term**
100 or less	$680	$9.38	$8.66	$7.95
101 to 250	$1,187	$8.57	$7.88	$7.19
251 to 300	$2,117	$6.48	$5.91	$5.34
301 to 400	$2,024	$6.19	$5.65	$5.10
401 to 500	$1,966	$6.01	$5.49	$4.96
501 to 750	$1,966	$5.44	$5.06	$4.81
751 to 1000	$1,885	$5.22	$4.85	$4.62
1001 to 2000	$3,498	$5.08	$4.85	$4.48
2001 or more	POA	POA	POA	POA

Internet Protection Hybrid charges

9.17 The following charges apply to your Internet Protection Hybrid service:

No. of users	**Monthly charge for two web gateways**
1500 or less	$734
1501 to 10000	$2,490
10001 or more	POA

No. of users	**Licence and support – monthly charge per user**	
	Licence and support (where we supply equipment)	**Support only (where you supply equipment)**
750 or less	$3.87	$2.86
751 to 1000	$3.53	$2.50
1001 to 1500	$3.20	$2.14
1501 to 2500	$3.20	$2.14
2501 to 5000	$2.87	$1.79

5001 to 10000	$2.53	$1.43

Email Security Audit charges

9.18 The following charges apply to your Email Security Audit service:

SERVICE CHARGE – ONCE OFF			
No. of users	**Inbound or outbound audit**	**Inbound and outbound audit**	**Inbound, outbound and internal audit**
499 or less	$1,800	$2,700	POA
500 to 1999	$2,333	$3,500	POA
2000 to 4999	$4,667	$7,000	POA
5000 to 9999	$8,000	$12,000	POA
10000 or more	POA	POA	POA

What other charges apply?

9.19 You can ask us to:

(a) help with installing and configuring your IPS; or

(b) do anything else that isn't included as part of your standard IPS charges,

and if we agree to your request, you must promptly pay us for the work we do.

9.20 The work that we do will be charged at our then current time and material rates, which we'll confirm at the time.

10 What service levels apply?

Which services have service levels?

10.1 The service levels in this section apply only to the Internet Protection Web and Internet Protection Mail service.

10.2 The relevant service levels don't apply during each period:

(a) your system configuration isn't compliant with all relevant standards and guidelines we tell you of from time to time;

(b) of planned maintenance;

(c) the applicable IPS aren't available due to an event beyond our reasonable control or due to acts or omissions of you or a third party; or

(d) the applicable IPS has been suspended in accordance with this section.

IT'S HOW WE CONNECT

How do I claim a rebate?

10.3 If we don't meet the service levels set out below, you may apply for a rebate (if specified below) but only if all of the following applies:

(a) you give us accurate and timely information we need to restore your IPS;

(b) you give us sufficient and timely access to the relevant premises or Facilities so we can try to restore your IPS;

(c) you haven't received a reasonably sufficient work-around solution, which enables you to continue to use your IPS; and

(d) in our reasonable view, the service level failure materially and detrimentally impacts your business (and if we ask, you must promptly give us any information needed to show this impact).

10.4 You must apply for a rebate under clause 10.3:

(a) by completing a rebate application form (which we can provide on request) and returning it to your Telstra representative; and

(b) within 5 Business Days of the end of the month, which the rebate claim relates to,

otherwise, you're not entitled to a rebate.

10.5 We'll let you know whether we agree if you're eligible for a rebate and if so, it will be calculated as set out further below.

10.6 The total amount of any rebate won't exceed the total monthly payment we receive for the affected IPS. The rebates set out below are your sole and exclusive remedy in connection with any service level failure.

How we measure service levels

10.7 We're solely responsible for measuring our performance of the applicable IPS against their relevant service levels.

10.8 We measure the relevant service levels 30 days after you first start using the service.

Platform availability service level

10.9 Platform availability is the percentage of time the applicable IPS platforms are available to you in the prior 12 months.

10.10 We aim (but don't guarantee) to achieve a platform availability target of 99.9% calculated over a 12 month period. If we don't meet this target, you may apply for a rebate of 5% of the relevant monthly service fees for each affected service per 30 minute period for which the target isn't met.

Internet Protection Mail performance service level

10.11 Performance for the Internet Protection Mail service relates to email traffic passing through that service. We aim (but don't guarantee) to meet the average standards set out in the table below. These standards are averages per message over a 3 month time period:

Traffic type	Average < than
Email traffic not scanned	30 seconds
Email traffic to which the anti-virus and anti-spam services are applied	60 seconds

10.12 If we don't meet the service level in the above table, you may apply for a rebate of 5% of the relevant monthly service fees for each affected service per 30 minute period for which the service level isn't met.

Internet Protection Mail accuracy service level

10.13 We aim (but don't guarantee) that the Internet Protection Mail service meets the following target service levels:

(a) 100% detection of known viruses;

(b) 0.0001% virus false positive capture rate;

(c) 99% spam detection rate;

(d) 0.0003% spam false positive capture rate;

(e) 100% email delivery target; and

(f) 100% email service uptime target.

10.14 If we don't meet the detection of known viruses service level, you may apply for a rebate as follows:

Incidents	Percentage credit of monthly service charge that relates to the impacted service(s).
< 2	20%
< 5	50%
> 5	100%
The above rebates don't apply where the email (for whatever reason), falls outside the standard scanning standards.	

10.15 If we don't meet the virus false positive capture rate service level, you may apply for a rebate as follows:

False positive	Percentage credit of monthly service charge that relates to the impacted service(s).
> 0.0001% but < 0.001%	20 %
> 0.001% but < 0.01%	50 %

IT'S HOW WE CONNECT

> 0.01% but < 0.1%	75 %
> 0.1%	100%

10.16 If we don't meet the spam detection rate service level, you may apply for a rebate as follows:

False negative	Percentage credit of monthly service charge that relates to the impacted service(s).
> 3%	20 %
> 8%	50 %
> 15%	75 %
> 20 %	100%

10.17 If we don't meet the email delivery target service level, you may apply for a rebate as follows:

Percentage service availability per calendar month	Percentage credit of monthly service charge that relates to the impacted service(s).
< 100% but > 99.0%	15%
< 99.0% but > 97.0%	30%
< 97.0% but > 95.0%	45%
< 95%	100%

Internet Protection Web performance service level

10.18 Performance for the Internet Protection Web service relates to web traffic passing through that service. We aim (but don't guarantee) to process and deliver web requests 99.999% of the total hours during every month you use the service, subject to the following:

(a) you're given both primary and secondary proxy addresses, so non-availability is measured only where both proxy addresses are simultaneously unavailable. Downtime is measured from the time of actual interruption of the Internet Protection Web service until the time that service is restored; and

(b) the service level only applies to downtime due in whole or in part to our inability to provide service to you, which are not attributable to planned maintenance.

10.19 If we don't meet the above performance service level, you may apply for a rebate as follows:

Monthly service availability	Percentage credit of monthly service charge that relates to the impacted service(s).
99.999 - 99.5 %	10%
99.49 - 99.0 %	20%
98.99 - 98.5 %	30%
98.49 - 98.0 %	40%

IT'S HOW WE CONNECT

97.99 - 97.5 %	50%
97.49 - 97.0 %	60%
96.99 - 96.5 %	70%
96.49 - 96.0 %	80%
95.99 - 95.5 %	90%
Less than 95.5%	100%

Internet Protection Web – false-positive web filtering rate

10.20 The false-positive filtering rate service level measures the percentage of URLs and domains blocked by the Internet Protection Web Service but based on your chosen categorisation policies, shouldn't have been blocked ("**Bad Blocks**"). For clarity, if a URL is in the "unclassified" category it will blocked if you've chosen to block all unclassified URLs.

10.21 The false-positive filtering rate is equal to:

100

x total number of Bad Blocks in a calendar month at all sites.

÷ total number of URLs scanned by the Internet Protection Web Service at all sites during the same calendar month

where the Bad Blocks are determined by us acting reasonably.

10.22 If the false-positive filtering rate is greater than or equal to 0.0004%, you may apply for a rebate equal to 10% of the monthly service charges for your impacted Internet Protection Web Service.

Internet Protection Web – false-negative web filtering rate

10.23 The false-negative filtering rate service level measures the percentage of URLs and domains that weren't blocked by the Internet Protection Web Service but based on your chosen categorisation policies, should have been blocked ("**Missed Blocks**"). For clarity, if a URL is in the "unclassified" category it will be blocked if you have elected to block all unclassified URLs.

10.24 False-negative filtering rate is equal to:

100

x total number of Missed Blocks in a calendar month at all sites.

÷ total number of URLs scanned by the web filtering service at all sites during the same calendar month.

where the Missed Block are determined by us acting reasonably.

IT'S HOW WE CONNECT

10.25 If the false-negative filtering rate is greater than or equal to 0.0004%, you may apply for a rebate equal to 10% of the monthly service fees for the impacted Internet Protection Web Service.

11 Minimum term and termination

What's the minimum term for the IPS?

11.1 You must obtain each:

(a) Internet Protection Hybrid service for a minimum term of 36 months; and

(b) other IPS (except for an Internet Protection Hybrid service) for a minimum term of at least 12 months.

11.2 Once your minimum term ends, it automatically extends on a month-to-month basis on the existing terms (including price). This continues until one of us gives the other at least 30 days' written notice that it wishes to terminate the term for that individual IPS.

11.3 If you cancel or terminate an IPS (other than for our breach) before the minimum term ends, you must pay us on request, the following early termination fee for each IPS:

(a) for an Internet Protection Hybrid service, 50% of A x B;

(b) for an Internet Protection Mail service, 25% of A x B;

(c) for an Internet Protection Web service, 70% of A x B; and

(d) for an Internet Protection Web and Mail Bundle, 50% of A x B:

A = the average monthly fees for the relevant IPS.

B = the number of months (or part of a month) remaining in the minimum term.

11.4 You agree that the early termination fees in this section are a genuine pre-estimate of our loss we're likely to suffer.

Terminating an IPS

11.5 You or we may terminate an IPS with at least 30 days' prior written notice. An early termination fee may apply, which we can confirm on request.

11.6 Without limiting our rights or remedies, we may suspend or terminate some or all of your IPS at any time if you breach any:

(a) term in this section; or

(b) any other obligation you have in connection with the IPS,

and we think the breach:

(c) can't be fixed or can't be fixed to our satisfaction; or

(d) can be fixed to our satisfaction and you don't fix it within 14 days of us telling you to do so.

11.7 If you breach any term in this section or any other obligation you have in connection with the IPS, you must promptly pay us for any remedial work (at our then current rates that we tell you at that time) which is needed because of your breach; and

11.8 If one of our suppliers suspends or terminates a service or component we need to provide your IPS, then we may suspend or terminate your IPS. If this happens, we'll try and give you as much notice as we reasonably can.

11.9 If we suspend or terminate an IPS for any reason, then you're responsible for all necessary configuration and other changes to your servers and network and to inform your Internet service provider of the need to reroute inbound email and web traffic.

12 Special meanings

12.1 The following words have the following special meanings:

AMP or Advanced Malware Protection has the meaning given in clauses 4.31 to 4.33.

Business Day means Monday to Friday (excluding local public holidays).

Business Hours are 8am to 5pm (AEST) on Monday to Friday (excluding local public holidays).

DKIM or **Domain Keys Identified Mail** refers to the digital signature based, email sender domain authentication and integrity system.

Email Security Audit is described in clause 7.1.

Facilities has the meaning given in clause 8.4(b).

Internet Protection Hybrid is described in clause 6.1 to 6.2.

Internet Protection Mail is described in clause 4.1.

IPS or **Internet Protection Services** has the meaning given in clause 2.1.

Internet Protection Web is described in clause 3.1.

Obsolete Equipment has the meaning given in clause 6.13.

PIM or **Passive Identity Management** is described in clause 3.30.

RBAC means role based access control.

SMTP means simple mail transfer protocol.

IT'S HOW WE CONNECT

This section was last changed on 27 April 2017.

IT'S HOW WE CONNECT