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

Contents

Click on the section you're interested in.

1 About this section

Words with specific meanings

Certain words are used with the specific meanings set out:

(a) on page 48;

(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 Internet Protection Services (or "**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.

No assignment or resupply

1.7 IPS aren't available to Telstra wholesale customers or for resale. You must not assign or resupply IPS to a third party.

We have to approve your requests

1.8 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

1.9 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) Secure Web;

(b) Secure Email;

(c) Secure Web and Secure Email;

(d) Internet Protection Hybrid;

(e) Email Security Audit;

(f) Professional Services; and

(g) Managed Services.

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.

Service not issue free

2.8 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, 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 Secure Web and Secure Email services 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.

What is the portal reporting service?

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

2.17 All reports for your IPS 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.

Unified portal (basic applications) service for Secure Web and Secure Email service?

2.18 The Secure Web and Secure Email services include a unified portal (basic applications) service.

2.19 This service aims to provide a unified security portal with applications for visibility, policy controls and reporting.

Additional reporting

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

Changes to your IPS

2.21 We can change any part of the IPS without telling you. Unless clause 2.22 applies, if the change materially and detrimentally affects your IPS we will only do so in accordance with the variation process set out in the General Terms of Our Customer Terms.

2.22 If you ordered your IPS on or after 1 Janaury 2023 and a change to your IPS:

(a) is not required by law, to prevent fraud or for security or technical reasons; and

(b) materially and detrimentally affects your IPS:

we will give you as much notice of the change as possible (dependent where applicable on notice provided to us by any third-party supplier of the service) up to a maximum of:

(a) 30 days for changes to the IPS; or

(b) 60 days if the IPS or any part of it is being exited from the market.

2.23 If our changes under clause 2.22 are materially detrimental to you, you can cancel your IPS within 30 days of the notice. In this case:

(a) you must pay us any usage or other charges (including once-off costs) incurred up to the cancellation date; and

(b) you do not have to pay us any other early termination charges (if applicable).

Help desk

2.24 You can access our help desk.

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

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

2.27 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 Secure Web (formerly 'Internet Protection Web')

What is the Secure Web service?

3.1 The Secure Web (formerly 'Internet Protection Web') service aims to provide security features for your web traffic.

3.2 The following Secure Web packages are available for you to chose from depending on your requirements:

SECURE WEB – Essential	
Feature	**Secure Web - Essential**
Secure portal RBAC	✓
Intelligent proxy	✓
Web filtering and File reputation	✓
Collective security intelligence	✓
Prevent malware, phishing, and C2 callbacks over any port	✓
Block high risk other security categories (cryptomining, newly seen domains, etc.)	✓
Stop acceptable use violations (up to 100 content categories), plus enforce SafeSearch	✓
DNS-layer control by security setting, content filtering, and customized block/allow list (domains)	✓
Proxy risky domains with customisable URL blocking and file inspection using Cisco Advanced Malware Protection (AMP) and anti-virus engine	✓
Customizable block pages and bypass options	✓
Real-time, enterprise-wide activity search & scheduled reports	✓
Identify targeted attacks with local vs. global activity report	✓
Application Discovery and blocking to combat shadow IT	✓
Log extraction or retention by Customer up to 30 days	✓
AnyConnect Roaming Security Module	✓
AnyConnect VPN Module	O

SECURE WEB – ADVANCE AND PREMIUM		
Feature	**Secure Web Advance**	**Secure Web Premium**
Secure Web Gateway		
Proxy and inspect web traffic (incl. decryption of SSL (HTTPS) traffic)	✓	✓
Enable web filtering by domain or category (SIG filtering by URL)	✓	✓
Create custom block/allow lists of domains	✓	✓
Create custom block/allow lists of URLs	✓	✓
Block files based on AV Engine and malware defense	✓	✓
Use malware analytics (sandbox) on suspicious files	500/day	Unlimited
Cloud Access Security Broker		
Cloud app discovery, risk scoring, blocking or activity controls	✓	✓
Scan and remove malware from cloud-based file storage apps	Two apps	✓
DNS-layer Security		
Block domains with malware, phishing, botnet, or other high-risk items	✓	✓
Cloud-delivered Firewall		
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols	✓	✓
Leverage layer 7 protection including an Intrusion Prevention System	O	✓
Data Loss Prevention		
Enable in-line DLP inspection and blocking capabilities to protect sensitive data	O	✓
Remote Browser Isolation		
Provide safe access to risky sites, web apps and all web destinations	O	O
XDR and Threat Intelligence		
Utilize SecureX cross product security data and automated response actions	✓	✓
Access Umbrella's deep domain, IP, and ASN data for rapid investigations	✓	✓
Remote User Protection		
AnyConnect Roaming Security Module	✓	✓
AnyConnect VPN Module	O	O

KEY:
✓ = Available with the package.
X = Not available with the package.
O = Optional add-on with the package for an additional monthly charge.

3.3 If you ordered your Secure Web service on or after 1 January 2023, during the minimum term you can also make up to two (2) Simple Changes to your service per month. A Simple Change is defined in clause 9 (below).

3.4 You acknowledge and agree the Secure Web service and packages are provided by a third-party who may make changes to the included features from time to time in accordance with clauses 2.21, 2.22 and 2.23.

Service Connection Work Package

3.5 You must take up a Service Connection Work Package for each Secure Web service you order. Your Service Connection Work Package is a once-off set up service and for Secure Web services will include:

(a) basic provisioning, activation and onboarding including (if required for Secure Web Advance or Premium) Cisco Meraki SD-WAN integration;

(b) basic testing and Secure Web service verification;

(c) up to one (1) hour of virtual training on use of the Secure Web service and portal; and

(d) Secure Web portal guide and online help documentation.

3.6 The once-off charge for the Servce Connection Work Package will be specified in your Service Order for your Secure Web service.

3.7 We (or our third parties) are to soley provide you with the Service Connection Work Package services. You must ensure that you and/or any other third-party do not perform all or part of the Service Connection Work Package services.

Any Connect Roaming Security Module

3.8 Your Secure Web service package includes an AnyConnect Roaming Security Module. This feature aims to provide secure remote user access to your internal network and Internet resources.

3.9 You must request the Any Connect Roaming Security Module for at least 5 users. The AnyConnect Roaming Security Module will also require you to install an endpoint agent provided with the service and may require integration with your Active Directory (AD).

3.10 You can also add the AnyConnect VPN Module for an additional cost (see further below at clauses 3.23and 3.24).

What is the centralised policy management service?

3.11 All Secure Web packages include a centralised policy management service. This 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 command and control call-back blocking service?

3.12 This Secure Web feature uses command and control call blocking. It aims to:

(a) stop connection to the attacker's server; and

(b) if infection occurs, it aims to stop data exfiltration and execution of ransomware encryption.

What is the IP layer enforcement service?

3.13 This Secure Web feature aims to stop:

(a) threats over all ports and protocol, (including direct to IP connections); and

(b) malware before it reaches your endpoints or network.

What is the intelligent proxy service?

3.14 This Secure Web feature aims to route requests to risky domains for deeper URL and file inspection.

What is the virtual appliance service?

3.15 This Secure Web feature provides a DNS forwarder function within your network and is needed to use the "active directory integration" service. It aims to:

(a) forward external DNS queries to the Secure Web service;

(b) route internal DNS queries to your configured internal DNS servers; and

(c) identify the source of DNS requests on your network.

Configuring your traffic to use Secure Web

3.16 To use the Secure Web service, you must ensure your external traffic is directed through the Secure Web service at all times.

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

3.18 You're responsible for configuring your systems to direct external traffic through the Secure Web service.

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

What are the Internet Protection Web service optional features?

3.20 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) Any Connect VPN Module;

(c) advanced active directory integration options; and

(d) log extraction or data retention.

What is the HTTPS inspection service?

3.21 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.

3.22 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 AnyConnect VPN Module Add-On?

3.23 You can add AnyConnect VPN Module to your Secure Web service for an additional monthly charge. This feature aims to provide secure remote user access to your internal network, hosted applications, and Internet resources.

3.24 The AnyConnect VPN Module will also require you to install an endpoint agent provided with the service and may require integration with your Active Directory (AD).

What is the advanced active directory integration service?

3.25 You can add an advanced active directory integration service for an addition once-off fee. This service allows authentication / identification by integration with active directories for policy control and reporting down to user group level.

What is the log extraction or data retention services?

3.26 This service aims to let you retain or extract web usage data for secure analysis.

3.27 You can request this service as a custom professional or managed service under clause 8 or 9 (below). The requirements and pricing for the log extraction or data retention service will be agreed under a Service Order .

4 Secure Email (formerly 'Internet Protection Email')

What is the Secure Email service?

4.1 The Secure Email (formerly 'Internet Protection Mail') service aims to provide security features for your email traffic.

Previous Secure Email Packages (not available after 22 January 2018)

4.2 If you take up a Secure Email service before 22 January 2018, you can choose from the "Essential", "Enhanced" or "Premium" package depending on your requirements:

SECURE EMAIL			
Feature	**Essential**	**Enhanced**	**Premium**
Anti-virus	✓	✓	✓
Email content control	✓	✓	✓
Anti-spam	✓	✓	✓
Forged Email filter	✓	✓	✓
C-level impersonation filter	✓	✓	✓
Email system failover	✓	✓	✓
Alerts on system unavailability	✓	✓	✓
Secure portal RBAC	✓	✓	✓
Centralised policy management	✓	✓	✓
Unified portal apps (basic apps)	✓	✓	✓
Trace app with 8 day replay	✓	✓	✓
Data loss prevention & risk app	✓	✓	✓
SPF filter (Email spoofing)	✓	✓	✓
DKIM filter (Email spoofing)	✓	✓	✓
Typo domain filter	✓	✓	✓
Office 365 Email security	✓	✓	✓
Email spooling	✓	✓	✓
URL filtering (basic)	✓	✓	✓
Two-factor authentication	✓	✓	✓
Self-release	✓	✓	✓
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
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.			

Current Secure Email Packages (available from 22 January 2018)

4.3 If you order a Secure Email service on and from 22 January 2018, you can order an "Essential" package which includes the following features:

SECURE EMAIL	
Feature	**Essential**
Anti-virus	✓
Email content control	✓
Anti-spam	✓
Forged email filter	✓
C-level impersonation filter	✓
Email system failover	✓
Alerts on system unavailability	✓
Centralised policy management	✓
Unified portal apps (basic apps)	✓
Trace app with 8 day replay	✓
Data loss prevention & risk app	✓
SPF filter (email spoofing)	✓
DKIM filter (email spoofing)	✓
Typo domain filter	✓
Office 365 email security	✓
Email spooling	✓
Self-release	✓
URL filtering (advanced)	✓
Two-factor authentication	✓
Secure portal RBAC (up to 6 roles)	✓

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

4.4 If you ordered your Secure Email service on or after 1 January 2023, during the minimum term you can also make up to two (2) Simple Changes to your service per month. A Simple Change is defined in clause 9 (below).

4.5 You acknowledge and agree the Secure Email service and packages are provided by a third- party who may make changes to the included features from time to time in accordance with clauses 2.21, 2.22 and 2.23.

Service Connection Work Package

4.6 You must take up a Service Connection Work Package for each Secure Email service you order. Your Service Connection Work Package is a once-off set up service and for Secure Email services will include:

(a) basic provisioning, activation, and onboarding;

(b) basic testing and service verification;

(c) up to one (1) hour of virtual training on use of the Secure Email service and portal; and

(d) Secure Email portal guide and online help documentation.

4.7 The once-off charge for the Servce Connection Work Package will be specified in your Service Order for your Secure Email service.

4.8 We (or our third parties) are to soley provide you with the Service Connection Work Package services. You must ensure that you and/or any other third-party do not perform all or part of the Service Connection Work Package services.

What is the anti-virus service?

4.9 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.

4.10 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?

4.11 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.

4.12 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.

4.13 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?

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

4.15 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?

4.16 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?

4.17 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?

4.18 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.

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

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

4.21 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?

4.22 The alerts on system unavailability service aims to:

(a) monitor the performance of an Secure Email service; and

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

What is the secure portal RBAC service?

4.23 The secure portal RBAC service aims to provide your authorised IT administrator with access to the online portal. If you signed up for your service on and from 22 January 2018, this service can provide such access to up to 6 of your authorised IT administrators.

What is the centralised policy management service?

4.24 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 trace application with 8 day replay service?

4.25 The trace application with 8 day replay service aims to offer advanced search and retrieval of inbound and outbound emails for a retrospective time period of up to 8 days.

4.26 If you renew or order your Secure Web service on or after 1 January 2023, a retrospective time period of up to 32 days will apply to this service.

4.27 You can also extend (at an additional cost) your included retrospective time period for the length of your minimum term (up to a maximum of 36 months).

What is the data loss prevention and risk application service?

4.28 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?

4.29 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.

What is the DKIM filter (email spoofing) service?

4.30 This service uses the industry standard "Domain Keys Identified email" ("**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?

4.31 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 email security service?

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

4.33 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?

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

What is the self-release service?

4.35 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.

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

What is the URL filtering (basic) service?

4.37 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).

4.38 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?

4.39 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.

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

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

4.41 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?

4.42 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 are the Secure Email service optional features?

4.43 You may also request one or more standard or custom optional services with the Secure Email service for additional monthly fees which we can confirm on request).

Standard optional features

4.44 The following standard optional features can be added for additional monthly fee:

(a) Advanced Malware Protection (AMP)

(b) Image Control Application; and

(c) E-Discovery & Archiving.

What is the advanced malware protection (AMP) service?

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

4.46 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.

4.47 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 image control application service?

4.48 This service aims to enforce your policies on non-business and offensive images being sent / received from your Emailboxes. 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 is the e-discovery and archiving service?

4.49 This service aims to store Emails and index, with added advanced search for an agreed time frame. This time frame is extended for the length of your subscription (up to a maximum of 36 months).

Custom optional features

4.50 The following custom optional features can be added for additional monthly fees which will be priced on application and provided on your request:

(a) 7-year archive with trace and replay

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

(c) Extended trace application (up to 36 months)

(d) Customised applications or email security capability

(e) Encryption

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

4.51 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?

4.52 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?

4.53 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 custom applications service?

4.54 We can help develop customised apps or any other email security feature on request if you need particular capabilities in reporting, policy setting and security.

What is the encryption service?

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

There are requirements and limitations to the service

4.56 The Secure Email 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).

4.57 You must have a registered domain name to use the Secure Email service.

4.58 You must appropriately configure your domain name system to use the Secure Email service. On request, we can provide technical information on how to do this.

4.59 The service assurance and network availability targets which apply to the Telstra Internet Direct service don't apply to the Secure Email service.

4.60 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, 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 Secure Email service will function for email messages which you haven't routed in the way we tell you to; or

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

Email queue lengths

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

4.62 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 Secure Web and Secure Email Bundle

5.1 The Secure Web and Email bundle is made up of an:

(a) Secure Web service – Essential package; and

(b) Secure Email service – Essential package.

5.2 The applicable terms for the Secure Web and Secure Email services apply to your Secure Web and Email bundle.

5.3 If you ordered your Secure Web and Email bundle on or after 1 January 2023, for each month of the term of your service you can make:

(a) up to two (2) Simple Changes to your Secure Web service; and

(b) up to two (2) Simple Changes to your Secure Email service per month.

A Simple Change is defined in clause 9(below).

5.4 You can only terminate your Secure Web and Email 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 dedicated or customised security for your web, email or other Internet traffic. It can be hosted remotely or on a dedicated on-premise solution with equipment.

6.2 If you order a dedicated on-premise Internet Protection Hybrid solution, this will include 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).

6.3 The Internet Protection Hybrid service's features depend on your requirements but may include some or all the following:

(a) acceptable use policy controls;

(b) reputation filtering;

(c) malware filtering;

(d) data security;

(e) spam protection

(f) phishing protection; and

(g) application visibility and control (web).

Internet Protection Hybrid equipment

6.4 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.

6.5 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.

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

6.7 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.

6.8 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).

6.9 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.

6.10 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.

6.11 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.

6.12 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.

6.13 If you don't deliver the equipment as required under clause 6.12(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?

6.14 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.

6.15 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 Professional Service for Secure Web and Secure Email

What Professional Services are available for Secure Web and Secure Email?

8.1 If you take up a Secure Web, Secure Email or the Secure Web and Email Bundle service you can also add one or more once-off professional service packages at the additional cost specified in your Service Order **("PS Package")**

8.2 A PS Package gives you up to four (4) hours of consultancy services which will be delivered remotely to help with set-up and use related capabilities for your Secure Web and/or Secure Email service. This may include activities such as assistance with installation, integration, configuration, and policy changes depending on your requirements.

8.3 Full details of the PS Packages you can choose from and what each package includes is specified in the Secure Web and Email Managed and Professional Services Guide which you can request from us.

Adding a PS Package

8.4 You can add a PS Package via a Service Order when you take up a new Secure Web, Secure Email or Secure Web and Email Bundle service or at any time during the minimum term for those services.

8.5 We will carry out your PS Package:

(a) before or after your Secure Web and/or Secure Email has been implemented depending on the selected PS package or use case; and

(b) unless you request otherwise, during Business Hours. Any work performed outside of Business Hours will be at an additional cost.

What we need from you

8.6 In order for us to provide your PS Package you must:

(a) appoint one representative to be the lead contact who has relevant technical knowledge and experience related to your requested PS Package;

(b) provide us with all the information, assistance and access to systems, materials or other personnel we reasonably request or that is otherwise necessary for the supply of the PS Package;

(c) ensure that any information you provide to us is accurate and complete; and

(d) obtain any consents or authorisations required (including from any third parties) in order for you to comply with this clause 8.6.

8.7 You acknowledge and agree that if you do not comply with clause 8.6 we may not be able to provide you with all or part of your chosen PS Package.

Completion and non-completion of PS Packages

8.8 We will notify you if:

(a) we are unable to complete all or part of your requested PS Package, in which case we will only charge you for the number of consultancy hours worked on your Service Order up to the date of notification. We will provide you with a bill credit for any consultancy hours charged in advance that were not completed under this clause (on a pro rata basis);and

(b) your request will take longer than four (4) hours consultancy hours included in your requested PS Package, in which case:

(i) you can choose to add an additional PS Package; or

(ii) if you do not add an additional PS Pacakage, we will perform the four (4) hours of included consultancy work only. In this case you agree and accept that our performance of the included consultancy hours is effective completion of your PS Pacakge.

9 Managed Services for Secure Web and Secure Email

What Managed Services are available for Secure Web and Secure Email?

9.1 When you order or during the minimum term of a Secure Web, Secure Email or Secure Web and Email bundle service, you can also add a managed service package for an additional monthly charge specified in your Service Order (**"MS Package**").

9.2 You can add the following MS Packages for the full or remaining minimum term of your Secure Web, Secure Email or Secure Web and Email bundle service via a Service Order:

(a) Management and provision of:

(i) up to two (2) Simple, two (2) Complex, and one (1) Emergency Change/s if added to either one of your Secure Web or Secure Email service; or

(ii) up to four (4) Simple, four (4) Complex and two (2) Emergency Changes if added to a Secure Web and Email bundle service; and/or

(b) A custom managed service for Simple, Complex and Emergency Changes the requirements and pricing for which will be agreed between the parties under a Service Order.

Change definitions

9.3 The following definitions apply to Secure Web, Secure Email and Secure Web and Email bundle services:

Change means a policy and/or configuration change for your Secure Web and/or Secure Email services which is either a Simple, Complex or Emergency Change.

Complex Change means a change which is not a Simple or Emergency Change to an existing or additional complex web or email filter or policy such as

(a) A change to an existing or additional web filter:

(i) Group which is a combination of two or more IP addresses, subnets, and multiple AD groups or a custom group such as a specific user or IP address

(ii) contains a combination of two or more domains, categories, application visibility or exceptions; or

(iii) Schedule that is the definition of hours and timing to allow specific hours and time zone access (if applicable).

(b) A change to an existing or additional email policy such as:

(i) a custom configuration for email quarantine release actions; or

(ii) configuration of LDAP directory integration.

(c) Any other change that in our reasonable opinion is a fundamental change to the nature of the service or is not a Simple or Emergency Change.

Emergency Change includes Simple or Complex changes that you require urgently and may be required, for example:

(a) due to being critical to your business operations;

(b) due to your organisation's or business' service interruption (this does not include faults or interruptions to your Secure Web or Secure Email service);

(c) in response to your security breaches; or

(d) required for organisation-wide vulnerability patching.

Simple Change means a change to:

(a) an existing or additional standard web or email filter that contains only pre-defined categories; or

(b) an email standard filter policy which includes changes to policy settings, global actions or for selected emailboxes.

Change requests and Service Levels

9.4 You can request a Change as part of your MS Package via the help desk (**Change Request**) during Business Hours.

9.5 You must:

(a) provide us with all the information, assistance and access to systems or personnel we reasonably request or that is otherwise necessary for us to complete your Change Request;

(b) ensure that any information you provide to us is accurate and complete; and

(c) obtain any consents or authorisations required (including from any third parties) for you to comply with this clause 9.5.

9.6 You acknowledge and agree that if you do not comply with clause 9.5 we may not be able to complete your Change Request.

9.7 We will notify you:

(a) if we are not able to complete all or part of your Change Request for any reason or because it is not available to you under your MS Package; or

(b) that we have received and can implement your Change Request.

9.8 Once we notify you under clause 9.7, we will aim to complete your Change Request within the following Service Level Targets:

Change	Service Level Target
Simple	2 Business Hours from when we confirm your Change Request can be implemented
Complex	8 Business Hours from when we confirm your Change Request can be implemented

Emergency	2 Business Hours from when we confirm your Change Request can be implemented

9.9 You acknowledge and agree the above Change service level targest for your MS Package are indicative targets only, which we aim and will use reasonable efforts to meet, but do not guarantee. Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we are not liable for failing to meet these targets.

When will IPS Managed Services be completed

9.10 We will supply the MS Package services and carry out our obligations under this clause 9 during Business Hours.

9.11 After Business Hours MS Package services or Changes may be available at an additional cost. We will notify you of the cost and availability when you request this service.

10 What are your obligations?

10.1 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.

10.2 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.

10.3 If you breach clause 10.2(i), we may immediately suspend all or part of your IPS until you rectify the issue to our satisfaction.

10.4 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.

11 What fees and charges apply?

How we charge you for your IPS

11.1 We will charge you for your IPS on a single monthly invoice for the charges incurred for the full month (and not on a pro-rata or use basis) and:

(a) in advance for PS Packages and Service Connection Work Packages; and

(b) in arrears for all other IPS.

11.2 The charges for your IPS are:

(a) included in this section (below); or

11.3 will be provided to you on your application or request and then agreed in your Service Order for the relevant IPS. We'll charge you for the total number of:

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

(b) users, which your Secure Web service or Internet Protection Hybrid service will scan.

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

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

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

If your registered usage changes, so will your fees

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

11.7 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.

11.8 If you reduce the registered usage of your IPS before the end of your minimum term, you will be charged an early termination fee equal to the actual costs and expenses that we have incurred or committed to in anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the cancellation, which will not exceed an amount calculated as follows:

(a) for a Secure Email service (including an optional add-on service), 25% of A x B;

(b) for a Secure Web service (including an optional add-on service), 70% of A x B; and

(c) for a Secure Web and Email Bundle, 50% of A x B.

A = the monthly fee for the current/previous registered usage minus (-) the new monthly fee for the reduced registered usage.

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

11.9 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.

11.10 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.

Secure Web charges

11.11 If you acquire the Secure Web service only, you must pay us the below:

(a) once off Service Connection Work Package charge; and

(b) monthly service charge.

11.12 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.

11.13 If you're acquiring the AnyConnect VPN Module service, an additional charge per end user per month applies to the monthly service charges. We can confirm this charge on request.

Secure Web charges

SECURE WEB ESSENTIAL – SERVICE CONNECTION WORK PACKAGE CHARGE (ONCE-OFF) WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018 TO 31 DECEMBER 2022	
No. of users	**Essential**
Between 5 and 49 users	$840
Between 50 and 99 users	$880
Between 100 and 249 users	$1,028
Between 250 and 299 users	$1,160
Between 300 and 399 users	$1,213
Between 400 and 499 users	$1,271
Between 500 and 749 users	$1,331
Between 750 and 999 users	$1,567
Between 1000 and 1999 users	$1,999
2000 users and above	POA

SECURE WEB ESSENTIAL – SERVICE CHARGE (MONTHLY) WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018UNTIL 31 DECEMBER 2022			
No. of users	**12 month term**	**24 month term**	**36 month term**
Between 5 and 49 users	$5.35	$5.06	$4.88
Between 50 and 99 users	$4.37	$4.14	$4.13
Between 100 and 249 users	$4.23	$4.11	$4.00
Between 250 and 299 users	$3.99	$3.86	$3.66
Between 300 and 399 users	$3.99	$3.86	$3.66
Between 400 and 499 users	$3.99	$3.86	$3.66
Between 500 and 749 users	$3.65	$3.36	$3.20
Between 750 and 999 users	$3.65	$3.36	$3.20
Between 1000 and 1999 users	$3.13	$2.93	$2.75
2000 users and above	POA	POA	POA

SECURE WEB ESSENTIAL – SERVICE CHARGE WHERE YOU SIGNED UP FOR OR RE-ORDERED YOUR SERVICE ON AND FROM 1 JANUARY 2023					
No. of users	**Connection Charge (Once-off)**	**Price Per user Per Month**			
		12 month term	**24 month term**	**36 month term**	**Month to Month (If applicable after the end of the minimum term)**
100 or less	$840	$5.75	$5.64	$5.52	$6.90
101 to 200	$1,092	$5.41	$5.30	$5.20	$6.49
201 to 300	$1,420	$5.09	$4.99	$4.89	$6.11
301 to 400	$1,845	$4.79	$4.70	$4.60	$5.75
401 to 500	$2,307	$4.51	$4.42	$4.33	$5.41
501 to 750	$2,768	$4.25	$4.16	$4.08	$5.10
751 to 1000	$3,045	$4.00	$3.92	$3.84	$4.80
1000 or more	POA	POA	POA	POA	POA

Secure Email charges

11.14 If you acquire the Secure Email service only, you must pay us the below:

(a) once off Service Connection Work Package charge; and

(b) monthly service charge.

SECURE EMAIL – SERVICE CONNECTION WORK PACKAGE CHARGE (ONCE OFF) WHERE YOU SIGNED UP FOR YOUR SERVICE BEFORE 22 JANUARY 2018			
No. of Email boxes	**Essential**	**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

SECURE EMAIL ESSENTIAL – SERVICE CHARGE (MONTHLY) WHERE YOU SIGNED UP FOR YOUR SERVICE BEFORE 22 JANUARY 2018			
No. of Email 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

SECURE EMAIL ENHANCED – SERVICE CHARGE (MONTHLY) WHERE YOU SIGNED UP FOR YOUR SERVICE BEFORE 22 JANUARY 2018			
No. of Email 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

SECURE EMAIL PREMIUM – SERVICE CHARGE (MONTHLY) WHERE YOU SIGNED UP FOR YOUR SERVICE BEFORE 22 JANUARY 2018			
No. of Email 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

SECURE EMAIL – SERVICE CONNECTION WORK PACKAGE (ONCE-OFF) WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018 TO 31 DECEMBER 2022	
No. of seats	**Essential**
Between 5 and 49 users	$2,133
Between 50 and 99 users	
Between 100 and 249 users	
Between 250 and 299 users	$2,423
Between 300 and 399 users	$2,664
Between 400 and 499 users	$2,931
Between 500 and 749 users	$3,224
Between 750 and 999 users	$3,547
Between 1000 and 1999 users	$4,344
2000 users and above	POA

SECURE EMAIL ESSENTIAL – SERVICE CHARGE (MONTHLY) WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018 UNTIL 31 DECEMBER 2022			
No. of seats	**12 month term**	**24 month term**	**36 month term**
Between 5 and 49 users	$4.05	$3.85	$3.65
Between 50 and 99 users	$3.65	$3.45	$3.30
Between 100 and 249 users	$3.25	$3.05	$2.90
Between 250 and 299 users	$2.88	$2.76	$2.58
Between 300 and 399 users	$2.88	$2.76	$2.58
Between 400 and 499 users	$2.88	$2.76	$2.58
Between 500 and 749 users	$2.48	$2.38	$2.26
Between 750 and 999 users	$2.48	$2.38	$2.26
Between 1000 and 1999 users	$2.14	$2.03	$1.94
2000 users and above	POA	POA	POA

SECURE EMAIL ESSENTIAL – SERVICE CHARGE WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 01 JANUARY 2023					
No. of Email boxes	**Service Connection (Once-off)**	**Price Per Month Per Email Box**			
		12 month term	**24 month term**	**36 month term**	**Month-to-Month (If applicable after the end of the minimum term)**
100 or less	$2,133	$4.92	$4.89	$4.58	$5.90
101 to 200	$2,423	$4.34	$4.21	$4.09	$5.21
201 to 300	$2,664	$3.65	$3.45	$3.30	$4.38
301 to 400	$2,931	$3.26	$3.22	$3.03	$3.91
401 to 500	$3,224	$2.88	$2.76	$2.72	$3.46
501 to 750	$3,547	$2.66	$2.55	$2.50	$3.19
751 to 1000	$4,344	$2.45	$2.38	$2.26	$2.94
1000 or more	POA	POA	POA	POA	POA

SECURE EMAIL ADD ON – SERVICE CHARGE (MONTHLY) FOR ADVANCED MALWARE PROTECTION WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018				
No. of seats	**12 month term**	**24 month term**	**36 month term**	**Month-to-Month (If applicable after the end of the minimum term)**
Between 5 and 49 users	$1.60	$1.51	$1.43	$1.92
Between 50 and 99 users	$1.39	$1.29	$1.26	$1.67
Between 100 and 249 users	$1.31	$1.26	$1.20	$1.57
Between 250 and 299 users	$1.19	$1.13	$1.06	$1.43
Between 300 and 399 users	$1.19	$1.13	$1.06	$1.43
Between 400 and 499 users	$1.02	$0.97	$0.92	$1.22
Between 500 and 749 users	$1.02	$0.97	$0.92	$1.22
Between 750 and 999 users	$1.02	$0.97	$0.92	$1.22
Between 1000 and 1999 users	$0.88	$0.82	$0.78	$1.06
2000 users and above	POA	POA	POA	POA

SECURE EMAIL ADD ON – SERVICE CHARGE (MONTHLY) FOR IMAGE CONTROL APPLICATION WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018				
No. of seats	**12 month term**	**24 month term**	**36 month term**	**Month-to-Month (If applicable after the end of the minimum term)**
Between 5 and 49 users	$1.04	$0.98	$0.93	$1.25
Between 50 and 99 users	$0.90	$0.84	$0.82	$1.08
Between 100 and 249 users	$0.80	$0.78	$0.77	$0.96
Between 250 and 299 users	$0.77	$0.73	$0.69	$0.92
Between 300 and 399 users	$0.77	$0.73	$0.69	$0.92
Between 400 and 499 users	$0.66	$0.63	$0.60	$0.79
Between 500 and 749 users	$0.66	$0.63	$0.60	$0.79
Between 750 and 999 users	$0.66	$0.63	$0.60	$0.79
Between 1000 and 1999 users	$0.56	$0.52	$0.48	$0.67
2000 users and above	POA	POA	POA	POA

SECURE EMAIL ADD ON – SERVICE CHARGE (MONTHLY) FOR E-DISCOVERY & ARCHIVAL WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018				
No. of seats	**12 month term**	**24 month term**	**36 month term**	**Month-to-Month (If applicable after the end of the minimum term)**
Between 5 and 49 users	$3.58	$3.22	$2.86	$4.30
Between 50 and 99 users	$3.05	$2.74	$2.44	$3.66
Between 100 and 249 users	$2.87	$2.58	$2.29	$3.44
Between 250 and 299 users	$2.69	$2.42	$2.15	$3.23
Between 300 and 399 users	$2.69	$2.42	$2.15	$3.23
Between 400 and 499 users	$2.69	$2.42	$2.15	$3.23
Between 500 and 749 users	$2.51	$2.25	$2.00	$3.01
Between 750 and 999 users	$2.51	$2.25	$2.00	$3.01
Between 1000 and 1999 users	$1.83	$1.70	$1.55	$2.20
2000 users and above	POA	POA	POA	POA

Secure Web and Email bundle charges

11.15 If you acquire the Secure Web and Secure Email service, you must pay us the below:

(a) once off Service Connection Work Package charge; and

(b) monthly service charge.

11.16 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.

11.17 If you're acquiring the AnyConnect VPN Module service, an additional charge per end user per month applies to the monthly service charges below. We can confirm this charge on request.

	SECURE WEB AND EMAIL CHARGES WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 22 JANUARY 2018 UNTIL 31 DECEMBER 2022				
No. of seats/users	**Connection charge (once off)**		**Service charge (monthly)**		
	Essential	**Enhanced**	**12 month term**	**24 month term**	**36 month term**
Between 5 and 49 users	$1,701	$6,317	$8.46	$8.03	$7.60
Between 50 and 99 users	$1,701	$6,317	$7.60	$7.22	$6.84
Between 100 and 249 users	$1,872	$6,691	$6.75	$6.41	$6.08
Between 250 and 299 users	$2,059	$7,089	$6.05	$5.89	$5.76
Between 300 and 399 users	$2,264	$7,515	$6.05	$5.89	$5.76
Between 400 and 499 users	$2,491	$7,968	$6.05	$5.89	$5.76
Between 500 and 749 users	$2,793	$8,451	$5.63	$5.54	$5.43
Between 750 and 999 users	$2,901	$8,904	$5.63	$5.54	$5.43
Between 1000 and 1999 users	$3,688	$10,008	$5.33	$5.14	$4.98
2000 users and above	POA	POA	POA	POA	POA

SECURE WEB AND SECURE EMAIL ESSENTIAL CHARGES WHERE YOU SIGNED UP FOR YOUR SERVICE ON AND FROM 1 JANUARY 2023					
No. of seats/users	**Connection Charge (once off)**	**Price Per Seat Per Month**			
		12 month term	**24 month term**	**36 month term**	**Month-to-Month (If applicable after the end of the minimum term)**
100 or less	$2,527	$9.60	$9.47	$9.09	$11.52
101 to 200	$2,988	$8.78	$8.56	$8.36	$10.53
201 to 300	$3,471	$7.87	$7.60	$7.37	$9.44
301 to 400	$4,060	$7.25	$7.13	$6.87	$8.70
401 to 500	$4,701	$6.65	$6.46	$6.35	$7.98
501 to 750	$5,368	$6.22	$6.04	$5.92	$7.46
751 to 1000	$6,281	$5.80	$5.67	$5.49	$6.96
1000 or more	POA	POA	POA	POA	POA

Internet Protection Hybrid charges

11.18 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

11.19 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?

11.20 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.

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

12 What service levels apply?

Which services have service levels?

12.1 The service levels in this section apply only to the Secure Web and Secure Email service.

12.2 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.

How do I claim a rebate?

12.3 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).

12.4 You must apply for a rebate under clause 12.3:

(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.

12.5 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.

12.6 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

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

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

Platform availability service level

12.9 The Secure Web and Secure Email platform availability is the percentage of time the applicable platforms are available to you in the prior 12 months.

12.10 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.

Secure Email performance service level

12.11 Performance for the Secure Email 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

12.12 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.

Secure Email accuracy service level

12.13 We aim (but don't guarantee) that the Secure Email 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.

12.14 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.	

12.15 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 %
> 0.01% but < 0.1%	75 %
> 0.1%	100%

12.16 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%

12.17 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%

Secure Web performance service level

12.18 Performance for the Secure 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 Secure 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.

12.19 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%
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%

Secure Web – false-positive web filtering rate

12.20 The false-positive filtering rate service level measures the percentage of URLs and domains blocked by the Secure 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.

12.21 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 Secure Web Service at all sites during the same calendar month

where the Bad Blocks are determined by us acting reasonably.

12.22 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 Secure Web Service.

Secure Web – false-negative web filtering rate

12.23 The false-negative filtering rate service level measures the percentage of URLs and domains that weren't blocked by the Secure 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.

12.24 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.

12.25 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 Secure Web Service.

13 Minimum term and termination

What's the minimum term for the IPS?

13.1 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.

13.2 Your minimum term will be specified in your Service Order for your IPS. Once your minimum term ends, it automatically extends on a month-to-month basis on the existing terms:

(a) including price if you signed up for service before 1 January 2023; or

(b) if you signed up for your IPS on or after 1 January 2023 we may, with at leat 30 days' written notice:

(i) remove discounts or other special pricing offered to you for the minimum term; and

(ii) charge you our then current month-to-month standard fees for the IPS service.

13.3 This month-to-month term will continue under clause 13.2 until one of us gives the other at least 30 days' written notice that it wishes to terminate the term for that individual IPS

13.4 If you cancel or terminate an IPS (other than for our breach) before the minimum term ends, you must pay us on request, an early termination fee for each IPS of an amount equal to the actual costs and expenses that we have incurred or committed to in

anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the cancellation, which will not exceed an amount equal to the following:

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

(b) for an Secure Email service (including an optional add-on service), 25% of A x B;

(c) for an Secure Web service (including an optional add-on service), 70% of A x B;

(d) for an Secure Web and Email Bundle, 50% of A x B; and

(e) for an MS Package, A x B.

A = the average monthly fees for the relevant IPS (which can be based on the registered usage).

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

13.5 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

13.6 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.

13.7 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.

13.8 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

13.9 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 or transfer you to a reasonably comparable alternative service. If this happens, we'll try and give you as much notice as we reasonably can. If we transfer you to a reasonably comparable alternative service and this has more than a minor detrimental impact on you, you may cancel your service without having to pay any early termination charges for that service.

13.10 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.

14 Special meanings

14.1 The following words have the following special meanings:

AMP or Advanced Malware Protection has the meaning given in clauses 4.45 to 4.47.

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

Business Hours are 8am to 6pm (AEST) on Monday to Friday (excluding local public holidays).

DKIM or **Domain Keys Identified Email** 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 10.4(b).

Internet Protection Hybrid is described in clause 6.1 to 6.3.

Secure Email is described in clause 4.1.

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

Secure Web is described in clause 3.1.

MS Package means the managed service packages available for Secure Web, Secure Email and the Secure Web and Email bundle services and described in clauses 9.1 and 9.2.

Obsolete Equipment has the meaning given in clause 6.14.

PS Package means the professionalservice packages available for Secure Web, Secure Email and the Secure Web and Email bundle services and described in clauses 8.1, 8.2 and 8.3.

RBAC means role based access control.

Service Order means:

(a) an application form or order for a new IPS or to vary, renew, reconfigure, or cancel an existing IPS; or

(b) a statement of work, between the parties for services or other deliverables.

Service Connection Work Package means the once-off set-up services:

(c) described in clause 3.5 for Secure Web services; and

(d) described in clause 4.6 for Secure Email services.

SMTP means simple Email transfer protocol.