Contents

Click on the section that you are interested in.

Our Customer Terms
Vulnerabilty Services

Certain words are used with the specific meanings set out in this Vulnerability Services section and in the General Terms of Our Customer Terms.

1 About this Part

1.1 This is Our Customer Terms for Vulnerability Services. Provisions in other parts of the General Terms of Our Customer Terms, may apply to your Vulnerability Service.

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

1.2 This part only applies if you have one or more Vulnerability Services.

1.3 If there is an inconsistency between this part and the other parts of the General Terms of Our Customer Terms, this part prevails to the extent of the inconsistency.

2 Vulnerability Services

Availability

2.1 The Vulnerability Services are not available to Telstra Wholesale customers or for resale or supply to a third party.

What are the Vulnerability Services?

2.2 Telstra's Vulnerability Services help you identify IT systems in your external or internal network that might be vulnerable to known threats from the Internet by scanning your network for known vulnerabilities and reporting on security vulnerabilities in the scanned network.

2.3 The service scans your nominated IP addresses and web applications (**network assets**) against a list of known vulnerabilities and produces a report about the security vulnerability of those network assets.

Vulnerability Scan

2.4 You may apply for the Vulnerability Scan service.

Optional Vulnernability Service Add-on

2.5 You may also apply for the following optional Vulnerability Service Add-on features:

(a) Internal Scans

(b) Additional Web Application Scans

(c) Zero-Day Scans

(d) Consultant Reporting

Vulnerability Assessment

2.6 You may request a Telstra Security Consultant to conduct one or more of the Vulnerability Services on your behalf and provide a customised report.

Minimum term

2.7 You must obtain your Vulnerability Service for a minimum term of 12 months or such longer term as agreed.

3 Vulnerability Scan

3.1 The Vulnerability Scan is scan of your nominated public facing IP addresses and web applications conducted remotely from the Internet (**external scan**) and assessed against a list of known vulnerabilities. A report of this assessment is provided to you.

3.2 The Vulnerability Scan consists of the following scans of your nominated network assets:

(a) Vulnerability Management (VM) scan

(b) PCI Compliance (PCI-DSS) scan

(c) Web Application Scans (WAS)

Vulnerability Management (VM) scan

3.3 The Vulnerability Management (VM) scan allows you to scan your nominated network assets for listed known vulnerabilities which assists you in discovering key security vulnerabilities and latest malware.

PCI Compliance scan

3.4 The PCI Compliance (**PCI Compliance**) scan allows you to scan your nominated network assets for compliance with the current version of the Payment Card Industry Data Security Standard (PCI-DSS) which regulates how credit card information is stored and used.

3.5 The Payment Card Industry Data Security Standard is an information security standard for organisations that handle cardholder information from debit and credit cards. The standard is designed to reduce incidents of credit card fraud by providing a compliance framework that sets a baseline compliance level .

3.6 A PCI Compliance scan does not constitute validiation of your compliance with PCI-DSS. You are still required to perform validation of PCI-DSS as it applies to you.

Web Application Scans (WAS)

3.7 The Web Application Scan (WAS) scan allows you to scan your nominated web applications (including Internet URLs) to enable the detection of a number of application vulnerabilities including SQL injection and cross site scripting.

3.8 The Web Application Scan (WAS) assists discovery of official and “unofficial” applications residing on your network. WAS detects applications that are vulnerable to issues including the OWASP Top 10, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and URL redirection.

3.9 The Web Application Scan provides automated application penetration testing applications across a list of known vulnerabilities.

4 Vulnerability Service Add-ons

4.1 Telstra’s Vulnerability Service Add-ons extend the capabilities of your Vulnerability Scan.

4.2 You must acquire a Vulnerability Scan in order to get a Vulnerability Service Add-on.

4.3 Other than the Consultant Report, if you select a Vulnerability Service Add-on, you must get this for the same period as your Vulnerability Scan.

Internal Scans

4.4 The Internal Scan is a scan of your nominated internal IP addresses and web application network assets conducted remotely using dedicated hardware or a virtual scanner inside one or more of your network segments (**internal scan**) and assessment against a list of known vulnerabilities. A report of this assessment is provided to you.

4.5 The Internal Scan conducts a Vulnerability Management (VM) scan on your nominated network assets.

4.6 We will provide you with any dedicated hardware scanner or virtual scanner (**scanner**) required to conduct an internal scan as described in clause 8.

4.7 You have the option to select a separate Internal Scan report, or request a single combined Internal Scan and Vulnerability Scan report.

Additional Web Application Scans (WAS)

4.8 For your Vulnerability Scan, you may apply for extra Web Application Scans (WAS) in addition to the included number of Web Application Scans in your selected Vulnerability Scan package.

Zero-Day Scans

4.9 For your Internal Scan, you may apply for a Zero-Day Scan in addition to the Internal Scan. This feature will enable you to identify vulnerable applications and provide you with the opportunity to quarantine it from the network until a patch or update is supplied by the developer.

4.10 The Zero-Day Scan allows you to scan your network assets for "zero-day" vulnerabilities based on Verisign iDefense. This scan provides a check of your applications and operating system against a list of zero-day vulnerabilities. Zero-day vulnerabilities are newly discovered vulnerabilities that application and operating system developers have not had time to address and patch. Once a patch is available, a vulnerability is no longer classed as a zero-day vulnerability.

Consultant Reporting

4.11 For your Vulnerability Scan and Internal Scan, you may apply for a Telstra Security Consultant to examine your report. The consultant reviews the output of your report and assists you to interpret the results and provides its own report. The Telstra Security Consultant's services are provided as an Optional Service under Security Consulting Services section of the OCT. Charges for this reporting is set out in this document.

5 Vulnerability Assessment

5.1 You may request a Telstra Security Consultant to conduct one or more of the Vulnerability Services on your behalf, consult with you about your security objectives and priorities and provide a customised report. The Vulnerability Assessment is provided on the terms of the Optional Service under the Security Consulting Services section of the OCT.

6 Online service portal

6.1 Unless specified otherwise, the Vulnerability Services are requested and carried out via a self service portal.

Online service portal

6.2 We will provide you with access to an online portal accessible through the Internet to configure, manage and request Vulnerability Services and access scan reports. We will provide you with means of authentication to enable you to access this online portal.

6.3 You are responsible for ensuring that you have a connection to the Internet to enable you to use the online service portal.

Qualys platform

6.4 The scans are conducted through the online service portal using applications that are hosted on a platform by Qualys Inc (**Qualys**) and, other than for Internal Scans, you will not be provided with any software.

Access to Qualys platform

6.5 You must appoint an account administrator to manage the portal and be your single point of contact in relation to it. You must nominate users that may login (**portal users**) and users that may review and respond to messages (**profile users**). You are responsible for the use of the portal (including the platform) by your users, and any messages sent by your users, regardless of your relationship with those users.

6.6 You may change the number of users and the availability of service functionality to users at any time by using the web management tools. You acknowledge that you are responsible for configuring the portal and platform for your users. You are responsible for ensuring that all user information is accurate and up-to-date.

Licence

6.7 Your access to the online portal is provided on a limited, non-exclusive, non-transferrable non-sublicenceable basis, and only for the purpose of using the Vulnerability Services.

Account

6.8 You may only use your account to conduct scans of the entity on the name of the account, or any entities within the same corporate group. If you wish to conduct scans for other entities, you must obtain and use a separate account in the name of that other entity.

Usernames and passwords

6.9 You must ensure that any usernames, passwords are protected from unauthorised use, and are responsible for any acts or charges incurred through misuse, unauthorised use or failure to comply with guidelines provided to you. You must immediately notify us if you become aware of any unauthorised use. You must indemnify us for all claims and liabilities associated with unauthorised use of your usernames and passwords.

Notices

6.10 Notices relating to the Vulnerability Service will be available on the alert message on the online portal.

7 Scans and reports

7.1 Your Vulnerablity Scan report will contain the detected vulnerabilities in order of importance for the scanned network assets nominated by you.

7.2 Unless otherwise stated, each Vulnerability Scan and Internal Scan will produce a separate report.

Configuration of your network

7.3 The Vulnerability Services will only scan those network assets which are nominated by you and which you (and your system) allow to be scanned. You are responsible for identifying and nominating the network assets to be scanned, and for configuring your systems to allow those network assets to be scanned (eg. removing firewalls).

Currency of scan reports

7.4 Scan reports represent a point in time scan of your network assets against a list of known vulnerabilities or standards (as applicable) at the time the scan was conducted. The list of known vulnerabilities and standards is continually updated, and this may impact on the currency of your scan reports. You are responsible for conducting your scans at appropriate intervals based on your security needs.

Regularity of scans

7.5 You may conduct as many scans as you wish for the number of network assets included in your package. You are responsible for setting up the regularity and timing of your scans.

Accessing reports

7.6 Scan reports are generally available via the online service portal once you have conducted the scan. For a Vulnerability Assessment, we will provide the report directly to you.

8 Scanners

8.1 If we provide you with dedicated hardware or a virtual scanner to conduct an Internal Scan, we will provide such number of scanners as included in your subscription package. You may licence or rent additional scanners as required.

8.2 We will procure our supplier to provide you with the scanner, and you agree to comply with the terms of use in this clause.

8.3 The scanner contains software enabling the supplier to manage and update the scanner remotely, including the ability to cancel or discontinue scanning via the scanner.

8.4 Unless otherwise agreed, you are required to install the scanners yourself.

Dedicated hardware

8.5 We grant you a limited, non-exclusive, non-transferable, non-sublicenseable right to use the software embedded in the dedicated hardware in executable code form only to operate the hardware in connection with the Vulnerability Service.

8.6 Title to the hardware does not pass to you. You must return any supplied hardware, at your cost and in good working order (subject to fair wear and tear), to us within 7 days of expiration or termination of your service. If you do not, we will charge you for it.

8.7 You are responsible for any damage to the hardware caused by you or a third party.

Virtual scanner

8.8 The virtual scanner is licensed to you on a limited non-exclusive, non-transferrable, non-sublicensable license to: (i) install and use the virtual scanner for the number of your nominated network assets for your internal business purposes and (ii) use and reproduce the relevant documentation provided for use in operating the virtual scanner and (iii) move the virtual scanner to a different virtualization platform or make one copy of the virtual scanner solely for backup or archival purposes.

8.9 Installation of the virtual scanner on more than one virtualization platforms may require the purchase of additional subscription licenses, which we may give at our discretion, and additional licences from your third party suppliers, which you are responsible for obtaining.

8.10 You may make copies of the relevant documentation in human readable form, provided that such copies are (a) complete and not edited or abridged and (b) include all copyright and other proprietary information and notices contained in the original.

8.11 The virtual scanner may contain software (**open source software**) that is subject to a license that permits users to modify these portions and redistribute the modifications (**open source license**). Your use of the open source software may be subject to the GNU General Public License V2 ("GPL") or the GNU Lesser General Public License ("LGPL"). Your use, modification and redistribution of the open source software is governed solely by the terms and conditions of the applicable open source license which can be found at (http://www.gnu.org/copyleft/gpl.html#SEC1). A list of the open source software and the applicable open source licenses including the relevant source code can be obtained by sending an email to us.

Scanners generally

8.12 You must not to reverse engineer, decompile, or disassemble any hardware or software that is embedded in or related to the Service, except as specified in this document.

8.13 You may not make any alteration, addition or modification to scanners, or open, disassemble or tamper with it in any fashion, or transfer possession to any third party.

8.14 Intellectual property in the dedicated hardware or virtual scanner is our property or the property of our suppliers, and does not pass to you.

9 Additional requirements

Internal use

9.1 You must only use the Vulnerability Services and any reports generated for your own internal use. Intellectual property in reports remains with us or our supplier (as applicable).

No fixes included

9.2 The Vulnerability Services scans only detect the relevant vulnerabilities and provide a report. The services do not test, exploit, manage, rectify or fix those vulnerabilities. You are responsible for taking any additional action required to address vulnerabilities identified in scan reports.

Known vulnerabilities

9.3 Scans of known vulnerabilities are based on a list of known vulnerabilities that are identified using data gathered from a number of sources, including major organisations at the time of the scan. Scans do not detect all known vulnerabilities that are known at the time of the scan.

Authority to scan

9.4 You represent to us and agree to only scan network assets to which you have been assigned by a recognised authority or have been authorised in writing by the relevant owner to scan. You may scan the network assets of a person within the same corporate group provided you have the relevant authority in writing. Other than this, you must not scan network assets of another party. You indemnify us for a breach of this clause 9.4.

Service interruption and back-up

9.5 You acknowledge and agree that:

(a) the scans may expose vulnerabilities or the presence of malware or other vulnerabilities and in some circumstances could result in the disruption of services or your network assets; and

(b) some optional features, including internal scans, involve substantial risk of Denial of Service (DOS) attacks, loss of service, hardware failure and loss or corruption of data. You are responsible for backing up all data contained in or available through the devices connected to the nominated network assets. We will not be liable for any loss of data that occurs during the conduct of the services.

Special Requirements

9.6 We will tell you of any restrictions or specific requirements that you will need to meet before we can provide the Vulnerability Services to you at the time you apply for your service. These requirements are in addition to any requirements specified in this section of Our Customer Terms or the Vulnerability Scan Responsibility Guide.

Trial

9.7 We may provide a trial of the Vulnerability Services to you for an agreed period. If we provide a trial, the terms set out in this document apply for the trial.

10 Term and termination

10.1 Upon the expiration of the minimum term, your Vulnerability Services we will cease to provide you with Vulnerability Services unless you renew for a term of not less than 12 months at least 14 days prior to the end of your minimum term,

10.2 If you cancel or terminate your Vulnerability Service, other than for our breach, before the end of the minimum term or renewed minimum term, we may charge you an early termination fee calculated as follows:

A x B x 75%

Where:

A = the monthly fees for the Vulnerability Service

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

10.3 You acknowledge that the early termination fee is a genuine pre-estimate of our loss we are likely to suffer.

Termination

10.4 Suject to clause 10.2, either of us may terminate a Vulnerability Service by giving the other at least 30 days' written notice.

10.5 Without limiting our rights or remedies, we may suspend the provision of the Vulnerability Service to you at any time where you materially breach these terms by:

(a) breaking any of the promises under this document; or

(b) not remedying a breach of these terms within 14 days of us telling you that you are required to rectify the breach.

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

10.7 If we suspend or terminate a Vulnerability Service for any reason, then you are responsible for making all necessary changes to your internal documentation, servers or network.

11 Telstra Managed Security Services

11.1 If you acquire Security Intelligence under the Telstra Managed Services section of Our Customer Terms, you may include the Vulnerability Services as a component of your Security Intelligence. Additional charges apply for this.

12 General

Professional services

12.1 Vulnerability Services do not include additional professional services. If you require any professional services (eg. to install scanners) or otherwise assist you in providing your Vulnerability Services, these will be provided on the terms set out in the Security Consulting Services of Our Customer Terms.

Additional reporting

12.2 We may provide additional reporting services with your Vulnerability Service.

Location of scanning and storage

12.3 The Vulnerability Services may take place at locations outside Australia. You acknowledge that data derived from scans of your network assets will be stored in the same location as the scanning equipment and will be subject to local laws of the scanning location.

Changes to delivery mechanism

12.4 We can change any part of the Vulnerability Services, which may include updates to the portal, platform and changes to comply with the law. We may make these changes without telling you if the change is likely to have no more than a minor detrimental impact on you.

Planned maintenance

12.5 We may schedule maintenance outages and change management windows to carry out planned maintenance and changes, which may cause temporary access to some or all of your Vulnerability Services. We will try to perform any maintenance that may disrupt the

service between 12.00 am and 6.00 am Sydney time. If we are required to perform emergency maintenance on the Vulnerability Service, then we will endeavour to inform you as soon as practical.

Liability

12.6 We do not promise to supply the Vulnerability Service at all times without any outages, faults or delays. We do not promise that we can fix all defects associated with the Vulnerability Services.

Security threat

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

Intellectual property rights

12.8 Except where otherwise specified, the intellectual property rights of the Vulnerability Service and any hardware or software used in connection with the Vulnerability Service are and will at all times remain our property or that of our licensors or suppliers (as the case may be).

Export restrictions

12.9 You may not download, export, or re-export any software or technical data received in connection with the Service (a) into, or to a national or resident of, any country to which the United States has embargoed goods, or (b) to anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. You represent and warrant that you are compliant with this clause.

13 Fees and charges

Payments and variations

13.1 The Vulnerability Services will be charged in advance on a single monthly invoice. All charges are payable within 30 days of the date of invoice or as otherwise agreed.

13.2 We will commence charging you for your Vulnerability Service from the date we advise you that configuration of your Vulnerability Service by us is complete.

Charges based on number of network assets

13.3 We will charge you for the Vulnerability Services based on the total number of IP addresses and web applicatons (as applicable) scanned, rounded up to next number in the table.

13.4 You must notify us, using the online tool if you change the number of network assets scanned. We will charge you the monthly charge applicable to the varied number of network assets rounded up to the applicable maximum number set out in the fees and charges table. You must not scan a number of network assets greater than the number covered by your registered usage.

13.5 You will not be able to reduce the number of network assets included in your package before the end of your minimum term.

13.6 We may issue additional invoices and adjust subsequent invoices to cover charges for the increase in the number of network assets scanned.

Scanning restictions

13.7 If you select for your Vulnerability Scan 150 or less IP addresses, you may select up to a maximum of 100 additional WAS and a maximum of 3,072 IP addresses for your Internal Scan.

13.8 If you select for your Vulnerability Scan 200 or more IP addresses, you must select a minimum of 150 additional WAS and a minimum of 4,000 IP addresses for your Internal Scan.

Minimum terms longer than 12 months

If you wish to acquire a Vulnerability Service for a minimum term of longer than 12 months, we will provide you with a price on application.

Vulnerability Scan charges

13.9 For the Vulnerability Scan service, we charge you as set out in the table below.

Number of IP addresses	Vulnerability Scan 12 month subscription	Monthly charge ex GST
8	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$283
16	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$396
32	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$567
64	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$907
96	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$1,304
128	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$1,701
150	For Vulnerability Management scan,PCI Compliance scan & 1 Web Application Scan (WAS)	$1,928
200	For Vulnerability Management scan,PCI Compliance scan & 2 Web Application Scan (WAS)	$4,811
300	For Vulnerability Management scan,PCI Compliance scan & 3 Web Application Scan (WAS)	$5,599
400	For Vulnerability Management scan,PCI Compliance scan & 4 Web Application Scan (WAS)	$6,255
500	For Vulnerability Management scan,PCI Compliance scan & 5 Web Application Scan (WAS)	$6,829
600	For Vulnerability Management scan,PCI Compliance scan & 6 Web Application Scan (WAS)	$7,346
700	For Vulnerability Management scan,PCI Compliance scan & 7 Web Application Scan (WAS)	$7,819
800	For Vulnerability Management scan,PCI Compliance scan & 8 Web Application Scan (WAS)	$8,258
900	For Vulnerability Management scan,PCI Compliance scan & 9 Web Application Scan (WAS)	$8,670

1000	For Vulnerability Management scan,PCI Compliance scan & 10 Web Application Scan (WAS)	$9,059
>1000	Details on Application	POA

Additional Web Application Scan Charges

13.10 If you acquire an Additional Web Application Scan, we will charge you an additional charge of $68 per month per.

Internal Scan Charges

13.11 For the Internal Scan, we charge you as set out in the table below.

Number of IP addresses	Internal Scan 12 month subscription	Monthly charge ex GST
256	For Vulnerability Management scan,includes 1 Scanner	$737
512	For Vulnerability Management scan,includes 1 Scanner	$907
1024	For Vulnerability Management scan,includes 1 Scanner	$1,474
1536	For Vulnerability Management scan,includes 1 Scanner	$1,814
2048	For Vulnerability Management scan,includes 1 Scanner	$2,268
2560	For Vulnerability Management scan,includes 1 Scanner	$2,495
3072	For Vulnerability Management scan,includes 1 Scanner	$2,722
4000	For Vulnerability Management scan,includes 1 Scanner	$12,385
5000	For Vulnerability Management scan,includes 1 Scanner	$13,536
6000	For Vulnerability Management scan,includes 1 Scanner	$14,560
7000	For Vulnerability Management scan,includes 1 Scanner	$15,489
8000	For Vulnerability Management scan,includes 1 Scanner	$16,346
9000	For Vulnerability Management scan,includes 1 Scanner	$17,136
10000	For Vulnerability Management scan,includes 1 Scanner	$17,886
20000	For Vulnerability Management scan,includes 1 Scanner	$23,727
30000	For Vulnerability Management scan,includes 1 Scanner	$28,015
40000	For Vulnerability Management scan,includes 1 Scanner	$31,554
50000	For Vulnerability Management scan,includes 1 Scanner	$34,593
>50000	POA	POA

13.12 For any additional dedicated hardware or virtual scanners not included in your subscription or for a Zero-Day Scan, we charge you as set out in the table below.

Item	Description	Monthly ex GST
Hardware Scanner	Rental of additional hardware scanners	$231
Virtual scanner	Licence of additional virtual scanner	$122
Zero Day Scan	Scan of Internal IP addresses for zero day vulnerabilities	$1,361

Consultant Report charges

13.13 Prices for your Consultant Report are set out in the tables below. These charges in addition to your Vulnerability Scan or Internal Scan charges.

Consultant Report – Vulnerability Scan	
Number of IP addresses scanned	Once Off

Consultant Report – Internal Scan	
Number of IP	Once Offex GST

	ex GST
8	$3,600
16	$3,600
32	$3,600
64	$3,600
96	$3,600
128	$3,600
150	$7,200
200	$7,200
300	$7,200
400	$7,200
500	$7,200
600	$10,800
700	$10,800
800	$10,800
900	$10,800
1000	$10,800
>1000	POA

addresses scanned	
256	$5,400
512	$5,400
1024	$5,400
1536	$5,400
2048	$5,400
2560	$5,400
3072	$7,200
4000	$7,200
5000	$7,200
6000	$7,200
7000	$7,200
8000	$7,200
9000	$7,200
10000	$10,800
20000	$10,800
30000	$10,800
40000	$10,800
50000	$10,800
>50000	POA

Vulnerability Assessment Service charges

13.14 Prices for your Vulnerability Assessment service will be provided to on request.

Professional services charges

13.15 Prices for professional service will be provided to on request.

14 Helpdesk

14.1 We will provide a help desk that is available 24 hours a day, 7 days a week. We will give you the details of the help desk when you request the Vulnerability Service.

14.2 You must report all faults with a Vulnerability Service to our help desk and give details of the fault and all other information necessary for us to investigate the fault.

14.3 If we are not able to resolve the fault, we may require Qualys to provide support.

14.4 If requested by you, we can arrange to provide on-site support for an additional charge.

14.5 You must not, and must not permit any other person, to attempt to rectify any fault or problem regarding the portal or platform without our prior written consent.

15 Service levels

About service levels

15.1 The service levels set out in this section apply to the Vulnerability Service

15.2 We will only commence monitoring the performance of a Vulnerability Service against the relevant service levels 30 days after the date you commence using that service.

15.3 The relevant service level will not apply to the Vulnerability Service:

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

(b) during each period of planned maintenance;

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

(d) during each period a Vulnerability Service has been suspended in accordance with these terms.

15.4 If we fail to meet the service levels set out below, you will be eligible for a rebate provided that you meet the following eligibility criteria:

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

(b) you give us sufficient and timely access to your premises or system so that we can attempt to restore your Vulnerability Service; and

(c) you have not been provided with a reasonably sufficient work-around solution which enables you to continue to use your Vulnerability Service.

15.5 In order to receive a rebate for service level, you must apply to us for that rebate within 5 working days of the end of the month which is the subject of the rebate claim.

15.6 To apply for a rebate, you must complete a rebate application form (we can provide this to you on request) and return the form to your relevant Telstra Representative.

15.7 We will let you know whether we agree that you are eligible for a rebate.

15.8 If you are eligible for a rebate, it will be calculated as set out below.

15.9 Subject to clause 15.12, the total amount of any rebate will not exceed the total monthly payment received by us for the affected Vulnerability Services. The rebates set out below are your sole remedy with respect to any failure to meet the service levels.

Measurement of service levels

15.10 We are solely responsible for measuring our performance of the Vulnerability Service against the relevant service levels.

Vulnerability Service - Platform Availability

15.11 We aim, but do not guarantee, to meet a service availability of the platform of 99.0% over 24 hours a day, 7 days a week, 365 days a year. Availability is measured on a quarterly basis.

15.12 If we do not meet the above service level you may apply for a rebate of up to 5% of the relevant monthly service fees for each affected service for which the service level is not met.

16 Special meanings

16.1 The following words have the following special meanings:

external scan has the meaning in clause 3.1.

internal scan has the meaning in clause 4.4.

IP means Internet Protocol.

known vulnerabilities are threats to a network from the Internet that have been identified and published as known vulnerabilities.

list of known vulnerabilities are a list of known vulnerabilities that is compiled using data gathered from a number of third party sources.

planned maintenance means maintenance that we or our suppliers have scheduled to perform on the systems we use to provide the Vulnerability Service.

URL means the uniform resource locator.