SECURITY CONSULTING SERVICES SECTION

CONTENTS

SECURITY CONSULTING SERVICES SECTION

Certain words are used with the specific meanings set in clause 11 and in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm

1 ABOUT THIS SECTION

1.1 This is the Security Consulting Services section of Our Customer Terms.

1.2 The General Terms of Our Customer Terms also apply to your Services. See section one of the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm for more detail on how the various sections of Our Customer Terms are to be read together.

2 SECURITY CONSULTING SERVICES

Our services

2.1 We provide a range of security consulting service packages.

2.2 The security consulting service packages you can ask us to provide are:

Policy Translation Services	Policy Design Services	Policy audit and optimisation services
Policy Translation – Firewall	Policy Design - Firewall	Policy audit and optimisation - Firewall
Policy Translation – IPS	Policy Design – IPS	Policy audit and optimisation – IPS
Policy Translation – Content Filtering	Policy Design – Content Filtering	Policy audit and optimisation – Content Filtering

2.3 We can also provide Change Request Assistance and additional consultancy services if you ask us to.

2.4 The security consulting services packages include fixed inclusions and have a pre-determined service scope. If you ask us to perform services outside the scope of the packages (including by requesting more changes, equipment, analysis or work than we include in the packages), then we will tell you and additional charges will apply if you still want us to perform the out-of-scope work. Some of the limits of the service are described in this Security Consulting Services Section of Our Customer Terms, and some are described in the Responsibilities Guide.

Availability

2.5 The Services are not available to Telstra wholesale customers or for resale.

3 WHAT IS POLICY TRANSLATION?

3.1 The Policy Translation service involves translating the policies that apply to your existing infrastructure, so that they will apply to different infrastructure.

What is included?

3.2 You can choose from one or more of the following three Policy Translation services. As part of those services:

(a) **Policy Translation – Firewall**: we'll provide the Policy Translation for your firewall, including:

(i) setting up the format for source firewall policies;

(ii) verifying completeness of source firewall policies;

(iii) translating your source firewall policy into a new firewall format policy;

(iv) translating source routing into a new firewall format;

(v) providing the new policy to your implementation team;

(vi) providing you with a guideline of the accepted configuration format for supported firewalls;

(vii) telling you if any policies could not be translated to the new infrastructure (for instance because the old policies were out of date, or because the languages were incompatible);

(viii) if you ask us to, advising how to extract information from your existing firewall (an extra cost will apply); and

(ix) if you ask us to, extracting policies from your existing firewall through remote access (an extra cost will apply);

(b) **Policy Translation – Intrusion Protection Service (IPS)**: we'll provide the Policy Translation for your IPS, including:

(i) translating the configuration;

(ii) implementing any customised signature;

(iii) providing the translated IPS to your implementation team;

(iv) providing you with a guideline of the accepted configuration format for supported IPS systems;

(v) telling you if any policies could not be translated to the new infrastructure (for instance because the old policies were out of date, or because the languages were incompatible); and

(vi) if you ask us to, extracting configuration from your existing IPS through remote access (an extra cost will apply); and

(c) **Policy Translation – Content Filtering**: we'll provide Policy Translation from existing content filtering system to another model, including:

(i) translating the policy;

(ii) providing the translated policy to your implementation team;

(iii) providing you with acceptable configuration formats for supported content filtering systems, as set out in the Responsibilities Guide;

(iv) telling you if any policies could not be translated to the new infrastructure (for instance because the old policies were out of date, or because the languages were incompatible); and

(v) if you ask us to, implementing the translated policy (an extra cost will apply).

What is not included?

3.3 We only provide Policy Translation services for particular types of infrastructure. We set out what these are in the Responsibilities Guide.

3.4 The following tasks aren't included in your Policy Translation services, unless we agree as an Optional Service at additional cost:

(a) project management for implementation of the translated policy;

(b) translating more than one platform or item of hardware;

(c) optimising rules;

(d) cleaning rules; and

(e) training.

3.5 The Policy Translation services are available in different packages, and there are numerical limits to the number of rules we will translate within each package. Those limits are set out in the table in section 8.1 below. If you ask us to exceed those limits, extra charges will apply.

Our assumptions

3.6 We assume in providing the Policy Translation Packages that:

(a) the infrastructure you want the policy translated to is 'like for like' with the existing infrastructure, meaning we think that it has:

(i) similar functionality;

(ii) the same number of interfaces;

(iii) the same traffic flow;

(iv) a recognised vendor; and

(v) similar technical capability;

(b) the existing service and the new service have similar architecture; and

(c) you don't have any additional routing, signature or policy requirements.

3.7 We also make various assumptions as set out in the Responsibilities Guide, depending on the type of infrastructure involved.

4 WHAT IS POLICY DESIGN?

4.1 The Policy Design services involve designing security policies for your firewall, IPS or content filtering system.

4.2 You can choose from one or more of the three following Policy Design services. As part of those services:

(a) **Policy Design – Firewall**: we'll design a firewall policy based on the requirements you tell us about, including:

(i) specifying the firewall device to be used;

(ii) creating a traffic and business requirements report; and

(iii) creating a policy based on your firewall model, including access control lists, NAT, PAT and routing;

(b) **Policy Design – IPS**: we'll design an IPS policy based on the requirements you tell us about, including:

(i) specifying the IPS device to be used;

(ii) gathering your requirements;

(iii) creating an IPS requirements report; and

(iv) creating an IPS ruleset based on your IPS model; and

(c) **Policy Design – Content Filtering**: we'll design a content filtering policy compatible with your security device based on the requirements you tell us about, including:

(i) specifying the device to be used;

(ii) gathering your requirements;

(iii) creating a 'Content Discovered' report; and

(iv) creating a content filtering policy.

Limitations

4.3 The Policy Design services are once-off services only, and are only available for particular hardware and architectures, as described in the Responsibilities Guide.

4.4 There are also numerical limits on the number of rules and signatures we will design as part of the services. Those limits are set out in the table in section 8.1 below. If you ask us to exceed those limits, extra charges will apply.

What is not included

4.5 The Policy Design services don't include professional services involved in implementing or managing the policies we create for you. You can ask us to provide the Optional Services of policy implementation, or coordinating and governance. These will be additional consultancy services and additional cost.

5 WHAT IS POLICY AUDIT AND OPTIMISATION?

5.1 Our Policy Audit and Optimisation service provides an audit of your current security policies and recommendations for improvements to those policies, based on the objectives you tell us about.

5.2 You can choose from one or more of the following three Policy Audit and Optimisation services. As part of those services:

(a) **Policy Audit and Optimisation – Firewall**: we'll assess your business and traffic requirements, audit your current firewall for alignment with those requirements and make recommendations about:

(i) unused rules;

(ii) overlapping or shadowing rules;

(iii) best-practice rules;

(iv) rules that may be adversely impacting device performance;

(v) rules needed to protect the firewall; and

(vi) rules that require modification;

(b) **Policy Audit and Optimisation – IPS**: we'll assess your business and traffic requirements, auditing your existing IPS against those requirements and make recommendations about:

(i) unused rules;

(ii) overlapping or shadowing rules;

(iii) best-practice rules;

(iv) rules that may be adversely impacting device performance;

(v) additional rules we recommend; and

(vi) rules that require modification;

(c) **Policy Audit and Optimisation – Content Filtering**: we'll assess your business and traffic requirements, auditing your current content filtering systems against those requirements and make recommendations about:

(i) unused rules;

(ii) overlapping or shadowing rules;

(iii) best practice rules;

(iv) rules that may be adversely impacting device performance;

(v) additional rules we recommend; and

(vi) rules that require modification.

5.3 If you acquire an ongoing service, we will conduct the audit twice each year at times we agree.

What is not included?

5.4 Our Policy Audit and Optimisation service does not include any modifications to rules or policies required to comply with legislative changes, it relates only to the technical substance of existing rules or policies. If you want us to perform services that consider, or are related to, legislative changes you must ask us whether we are prepared to do that as an Optional Service.

Limitations

5.5 Each service is separate, and doesn't involve a review of the other aspects of your system. For instance, a firewall review doesn't consider your IPS. For a review of all aspects of your system, you'll need to buy multiple services.

5.6 Your services have the following limitations:

(a) **Policy Audit and Optimisation – Firewall**: this applies to one firewall only, is once-off only (unless you buy a recurring service) and is available in the following denominations:

(i) small – where total rules, NAT routing and objects do not exceed 50;

(ii) medium – where total rules, NAT, routing and objects do not exceed 200; and

(iii) large – where total rules, NAT, routing and objects do not exceed 500;

(b) **Policy Audit and Optimisation – IPS**: the service applies to one IPS and up to 10 customised signatures, and is once-off only (unless you buy a recurring service); and

(c) **Policy Audit and Optimisation – Content Filtering**: this applies to one device only, and is a once-off service only (unless you buy a recurring service).

Optional services

5.7 You can ask us to provide Optional Services. The Optional Services for Policy Audit and Optimisation are:

(a) policy implementation; and

(b) change request review, completion and submission.

5.8 Extra charges apply for the Optional Services, and these are set out below.

Our assumptions

5.9 If we provide the Policy Audit and Optimisation services, we make various assumptions about your environment and architecture, as set out in the Responsibilities Guide.

6 CHANGE REQUEST ASSISTANCE AND OPTIONAL SERVICES

Change Request Assistance

6.1 You can request Change Request Assistance for any of your Services. Change Request Assistance comprises small amendments to other Services. We will tell you whether a

change that you request is Change Request Assistance, or a bigger job that will be performed as an Optional Service.

6.2 There are numerical limits that apply to each level of Change Request Assistance. Those limits are set out in the table in section 8.1 below. If you ask us to exceed those limits, then we will treat your request as a request for Optional Services.

Optional Services

6.3 You may request additional consultancy Optional Services from time to time.

6.4 We perform these optional services on a time and materials basis, and we'll give you the relevant rates when you apply for Optional Services.

6.5 Without limiting the range of services you can ask for, the following services are available as Optional Services:

(a) Policy Translation service – advising on how to extract information from your firewall, and extracting policies from your firewall or IPS through remote access; and

(b) Policy Design service – implementing or managing the design we prepare for you; and

(c) for Policy Audit and Optimisation:

(i) policy implementation;

(ii) change request governance and coordination; and

(iii) recurring services (twice-yearly audits).

7 SERVICES

7.1 Your application form will set out the details of the Services you've chosen.

7.2 We'll perform the Services you choose, and deliver the Deliverables to you.

7.3 We aim to meet the scheduled timeframes and delivery dates set out in your application form but cannot guarantee to do so. The time estimates in your application form are based on our previous experience, assumptions as to the nature of your internal environment, the availability of our consultants at the time of contract and the timeliness of your inputs and materials. As a result, any indications we give about delivery dates are only estimates and may change.

Your responsibilities

7.4 We need you to provide various inputs and do various things in order for us to perform the Services. These are different for each Service, and are set out in our Responsibilities Guide. We make the Responsibilities Guide available at http://www.telstra.com.au/customer-terms/business-government/data-services/security-consulting-services/index.htm

7.5 The Responsibilities Guide may change over time and it is up to you to make sure you have the latest version.

7.6 There are also general inputs we need from you no matter what Service you've asked us to provide. These are that you have to:

(a) provide enough sufficiently skilled staff members to support the Service, including a

key point of contact;

(b) provide a suitable work area for our staff when they are on your premises;

(c) give us any data, equipment or environmental facilities that we reasonably ask for;

(d) give us complete information regarding your processes, systems, application and network structures, including any future changes; and

(e) get all necessary authorisations and permissions for us to perform the Services. This may include from any person providing you with web hosting services, IT support services, cloud computing facilities or firewall management services.

7.7 If your particular environment involves special requirements or extra inputs from you, then these will be set out in your application form. These are on top of your responsibilities set out in the Responsibilities Guide or Our Customer Terms.

7.8 You must provide all materials and inputs by the dates specified in your application form or, where no dates are specified, when we tell you.

7.9 We won't be responsible for any delay or increase in cost as a result of you not doing anything you have to do. It may also mean that we can't provide your chosen Services at all.

Title and risk

7.10 Risk in a Deliverable passes to you when we deliver the Deliverable to you.

7.11 Property in and title to a Deliverable (excluding any intellectual property rights in a Deliverable) stays with us until you've paid us in full for that Deliverable.

Change management

7.12 Either you or we may ask for changes to the scope of Services or the Deliverables we are providing to you.

7.13 If we both agree on the proposed changes then we'll provide you with a document setting out the impact of the changes on the scope of your Services (including price, Deliverables and resources) unless these details are already set out in your change request.

7.14 If we reasonably consider that we'll need to undertake material effort to analyse and document the impact of the changes, then we may charge you for doing this work. We'll agree the prices for that with you separately before starting.

7.15 If you agree on the impacts of the change request, we'll perform the Services as varied by the requested change.

Warranties and liability

Australian Consumer Law

7.16 If you are a consumer as defined in the Australian Consumer Law, our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

7.17 We aim to, but can't guarantee, that each Deliverable will be free from defects or errors. Also, we can't guarantee that the Services will produce particular results or outcomes for you (such as achieving external certification, accreditation or industry standards). In particular, internet policies and security can't detect every possible limitation or fraudulent activity, can't guarantee that your systems will operate in an error-free way, or that they'll be safe from malicious attack.

7.18 You have to assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

Risks and permissions

7.19 You acknowledge that:

(a) the Services may result in interruptions, loss and damage to you, including to your computer systems, networks, websites, software, hardware, internet connections and data;

(b) security testing is inherently risky and carried out over public networks, which may result in unexpected outcomes like system crashes or the inadvertent disclosure of information;

(c) as part of some of the Services, we actively attempt to breach security controls and gain access to your systems, which may be criminal activity if we did it without your permission, so you are giving us that permission throughout the term of the services;

(d) if any of our activities are reported to an external body or authority, you'll do everything necessary to make sure that body is aware you authorised the activities involved in the Services; and

(e) our Services are based on information you give us and the infrastructure you have in place at the time we perform the Services, and don't apply to the extent the information is incorrect or the infrastructure changes.

We don't accept responsibility for your actions

7.20 We don't accept responsibility or liability for defects in a Deliverable that result from your inputs and/or materials or that are caused by misuse of or intentional damage to the Deliverable (other than by us).

7.21 We don't accept liability for our Services to the extent caused or contributed to by you.

7.22 Except under section 7.16 and to the maximum extent permitted by law, we're not liable to you for the Services, including the matters set out in sections 7.17 to 7.21, unless we've been negligent or deliberately breached our promises to you.

Intellectual property rights

7.23 As between you and us, we retain all intellectual property rights in and to our material which we incorporate into your Deliverables and any material we develop for you in carrying out the Services.

7.24 Unless otherwise agreed in writing, we grant you a perpetual, non-exclusive, non-sub-licensable and non-transferable licence in Australia to use, adapt and reproduce solely for your internal business purposes our material which is incorporated into a Deliverable and any material we develop for you in carrying out the Services.

7.25 Unless otherwise agreed in writing, the Services and any Deliverables are provided for your benefit only. You must not use them for a third party's benefit or allow a third party to use them.

Our personnel

7.26 Where our personnel perform the Services at your premises, you have to ensure that your premises comply with all applicable health, safety, environment and community laws and regulations.

7.27 You have to obtain any consents and pay any site access and induction charges necessary so our personnel can access your premises for the purposes of providing you the Services.

8 CHARGES AND SERVICE SCOPE

8.1 The charges for the Services (and where relevant, numerical limitations on service inclusions) are set out in the table below.

Service	Charges (GST-exclusive)
Policy Translation	
Firewall	
Small (up to 50 rules)	$2,700
Medium (up to 200 rules)	$4,500
Large (up to 500 rules)	$7,200
IPS (up to 10 customised signatures)	$2,700
Content Filtering	$3,600
Policy Design	
Firewall (up to 100 rules)	$7,200
IPS (up to 10 customised signatures)	$3,600
Content Filtering	$3,600
Policy Audit and Optimisation	
Firewall – once off	
Small (up to 50 rules)	$5,400
Medium (up to 200 rules)	$9,000
Large (up to 500 rules)	$12,600
IDS – once off	$1,440

SECURITY CONSULTING SERVICES SECTION

Service	Charges (GST-exclusive)
Content Filtering – once off	$7,200
Firewall – recurring	
Small (up to 50 rules)	$6,480 per year
Medium (between 50 and 200 rules)	$10,800 per year
Large (between 200 and 500 rules)	$14,400 per year
IDS - recurring	$1,440 per year
Content Filtering - recurring	$7,200 per year
Change Request Assistance	
Change Request: review, completion and submission	
Small (up to 4 change requests)	$3,600
Medium (up to 10 change requests)	$7,200
Large (up to 20 change requests)	$14,400
Optional Services	
All Optional Services	Price on application

8.2 You have to pay us the charges for the Services.

8.3 You also have to reimburse us for out-of-pocket expenses reasonably and actually incurred by us in performing the Services, as long as we:

(a) first obtain your verbal approval for each expense; and

(b) produce a valid invoice or receipt when claiming the expense.

Charges for ongoing services

8.4 The Policy Audit and Optimisation service is available as an ongoing service. The term of your Service is set out in your application form. We'll fix the charges for these Services for the Initial Term (as set out in your application form).

8.5 At the end of the Initial Term, we'll keep supplying the Services to you on a month-to-month basis until you tell us to stop, but the charges will revert to our then current charges for the relevant Services.

9 SERVICE LEVEL TARGETS

9.1 We try to meet the following service level targets when providing the Services. They are estimates only and we're not liable to you if we don't meet them.

9.2 Timeframes start from when we acknowledge receiving the request.

9.3 The timeframes are suspended for any period during which we're waiting for you to provide us with information or access to your equipment or sites, or for any matter outside our reasonable control.

9.4 There are no service level targets for the Optional Services.

Policy Translation

Deliverable	Target
Order Acknowledgment	24 hours
Initial Assessment of viability	48 hours
Migrated Policies Report	3 days from commencement of assessment
Policies extracted based on remote access availability (if chosen)	5 business days
Migrated policies implemented based on remote access availability (if chosen)	10 business days

Policy Design

Deliverable	Target
Order Acknowledgment	24 hours
Initial Assessment of viability	48 hours
Report	3 business days after initial requirement analysis
Firewall Requirements Report	
IPS Requirements Report	
IPS Requirements Report	
Ruleset	3 business days from date on which report is provided
Firewall ruleset	
IPS ruleset	
Content filtering ruleset	

Policy audit and optimisation

Deliverable	Target

Order Acknowledgment	24 hours
Initial Assessment of viability	48 hours
Optimisation report duration	3 business days from commencement of assessment

10 GENERAL

Confidentiality

10.1 You and we will treat as confidential information all information provided by the other relating to the provision of the Services including:

(a) your application form; and

(b) technical, operational, billing, pricing and commercial information in relation to the supply of the Services.

10.2 Neither you nor we will disclose the other's confidential information to any person except:

(a) to our respective employees, lawyers, accountants and sub-contractors on a 'need-to-know' basis as long as they first agree to observe the confidentiality required under these terms;

(b) with the other's prior written consent;

(c) if required by law, any regulatory authority or stock exchange; or

(d) if it's in the public domain.

10.3 If you think you need to disclose any detail about our Services to a third party in order to get their permission for us to provide the Services, you have to tell us first and not proceed unless we've approved the disclosure.

10.4 The confidentiality obligations are subject to your acknowledgement of the inherent dangers of public networks, as set out in clause 7.19(b).

Responsibility for your inputs

10.5 You're responsible for any loss, damage, liability, costs or expenses we incur because of a claim that any inputs or material you provided or our use of them providing you Services infringes the intellectual property rights of any person.

Indemnity

10.6 You indemnity us against all Loss we incur as a result of any claim by a third party about or in any way associated with the Services.

10.7 The indemnity doesn't apply to any Loss that's caused by our negligent, wrongful or wilful breaches of these terms.

Your rights to cancel your Services

10.8 You may cancel your service at any time by giving us at least 14 calendar days prior written notice (or a different period if it is specified in your application form). We'll cease work in

accordance with that notice. We'll charge you for all work performed up to the date your cancellation takes effect, based on our then current fee for service hourly rates.

11 SPECIAL MEANINGS

11.1 The following words have the following special meanings:

Change Request Assistance has the meaning given in section 6.1.

Deliverables means any output which we provide to you as a result of the Services, including any reports, documents, recommendations or policies, whether in physical or electronic form.

Initial Term means the initial term of your Service, as set out in your Application Form.

IPS means intrusion protection service.

Loss means any and all losses (direct, indirect, consequential or otherwise), costs, expenses (including legal expenses), liabilities and claims, howsoever arising and whether under contract, tort (including negligence) statute or otherwise.

NAT means native address translation.

Optional Services mean services described in section 6.5, or described elsewhere in this section of Our Customer Terms as Optional Services.

PAT means port address translation.

Policy Audit and Optimisation means the services described in section 5, excluding any Optional Services.

Policy Design means the services described in section 4, excluding any Optional Services.

Policy Translation means the services described in section 3, excluding any Optional Services.

Responsibilities Guide means the guide of that name that we produce relating to the Services, as amended from time to time.

Services means the security consulting services described in this section of Our Customer Terms.