IT'S HOW WE CONNECT

# Customer Responsibilities Guide

# MANAGED SECURITY SERVICES

August 2017

# RESPONSIBILITIES GUIDE

# 1. ABOUT THIS GUIDE

There are a number of terms, conditions, requirements, roles and responsibilities associated with the purchase and use of Telstra's Managed Security Services (**MSS**) solution.

The guide outlines both your and our roles and responsibilities regarding each MSS solution.

Requirements are split according to:

- Security Monitoring
- Security Intelligence
- Managed Next Generation Firewall bundle
- Managed Firewall
- Managed Intrusion Protection Service (IPS)

This guide is the companion document to the Managed Security Service section of Our Customer Terms, and your application form.

## 1.1 REQUIREMENTS – NEW CUSTOMERS

If you are a new MSS customer, you are expected to manage and use your MSS solution according to the requirements outlined in this guide.

If you choose not to follow these requirements, we will not be responsible for any loss or inconvenience experienced if your MSS solution is disrupted. In this circumstance, we may charge you additional fees in order to fix your MSS solution.

## 1.2 REQUIREMENTS – ALL CUSTOMERS

You are required to provide us with all applicable information, data, consents, authorisations, decisions and approvals in order activate service requests.

You can make changes to your MSS solution using the Telstra Security Services Portal.

It is your responsibility to identify any moves, adds or changes relevant to your MSS solution and submit the appropriate requests via the Telstra Security Services Portal.

You are also required to identify when you need assistance from your assigned Telstra account executive and submit the appropriate requests.

## 1.3 OUR REQUIREMENTS

We will provide the MSS solution according to the requirements outlined in this guide.

Our services are backed by service targets regarding availability and performance so you get the most out of your MSS solution.

We will provide service support and notify you of any service changes and let you know when a service request has been completed.

## 1.4 KEEPING YOUR CONTACT DETAILS UP-TO-DATE

From time-to-time we will need to get in contact with you regarding your MSS solution, so it's important that you keep your organisation's details up-to-date.

As an MSS customer, you need to ensure that the following contact details are correct and kept up-to-date:

**Commercial contact**: the authorised staff member who acts on your business's behalf regarding all commercial matters associated with your MSS solution. Note: your Telstra account executive may call these contacts the 'primary contact' when buying MSS solutions on your behalf.

**Technical contact:** the authorised person who answers any technical questions associated with your MSS solution on your behalf.

You can update your contact details via the Telstra Security Services Portal.

## 1.5 RECORDING YOUR SERVICE DETAILS

As an MSS customer, it is important that you record your services details below within the table, as this information is used to identify your device when logging an assurance call with Telstra.

| FIELD NATIONAL NUMBER | DEVICE NAME | DEVICE LOCATION |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 2. GENERAL

This section is applicable to all MSS Security Services set out below.

- Security Monitoring
- Security Intelligence
- Managed Next Generation Firewall bundle
- Managed Firewall
- Managed IPS

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| If you believe we have not satisfactorily completed a service or product installation, inform us within five business days of completion. | | ✓ |
| Report any faults with your products through the Telstra Security Services portal or via the Telstra helpdesk. | | ✓ |
| Monitor and respond to security alarms relating to the relevant service target as set out in Our Customer Terms. | ✓ | |
| Provide updates on the progress of all reported faults within the relevant service target as set out in Our Customer Terms. | ✓ | |

## 3. DEPLOYMENT ACTIVITIES

Following the signing of your agreement with us, a Project Manager or Technical Designer will contact you to begin the applicable deployment process set out below. Your assigned Project Manager or Technical Designer will remain your single point of contact until your MSS solution is live and the MSS Operations team can assume management control of your devices.

3.1 The following process applies to:

**Security Intelligence**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Plan your MSS solution deployment, including the collection and verification of information essential to the installation of your service | ✓ | |
| Provide a network diagram and other relevant information | | ✓ |
| Email a pre-installation checklist to you, and schedule a conference call to clarify each step and explore potential complexities | ✓ | |
| Prepare a deployment form for you to fill in based on information obtained during the pre-installation conference call | ✓ | |
| Check your internal and external networks by referencing your network diagrams, and document any key items such as routers, servers, network protocols, and IP addresses etc | ✓ | |
| Upon request provide the required policy and network information to us within the deployment form (if needed) | | ✓ |
| Provide the required security and outage contact information within the deployment form | | ✓ |
| Collect and compiling any remaining installation information that may be required into the deployment form from you | ✓ | |
| Approve the detailed design | | ✓ |
| Configure shared infrastructure, including VPN tunnel to receive your logs (and your security events if needed) | ✓ | |
| Apply the default correlation policy to your security events if applicable | ✓ | |
| Test basic functionality and connectivity to your device | ✓ | |
| Provide detailed information to Telstra for the formal test plan to test functionality and connectivity to your security device to ensure we are receiving your log data and your security events | | ✓ |
| Execute formal test plan in conjuction with you to test functionality and connectivity to your applications for final sign off | ✓ | ✓ |

| | | |
|---|---|---|
| Prepare for transfer from the deployment team to MSS Operations team | ✓ | |
| Introduce our customer security portal website | ✓ | |
| Formally transfer support to the MSS Operations team and host a transition call with you and your team | ✓ | |

3.2 The following deployment process applies to**:**

**Managed Next Generation Firewall bundle**
**Managed Firewall**
**Managed IPS**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Plan your MSS solution deployment, including the collection and verification of information essential to the installation of your service | ✓ | |
| Provide a network diagram and other relevant information | | ✓ |
| Email a pre-installation checklist to you, and schedule a conference call to clarify each step and explore potential complexities | ✓ | |
| Prepare a deployment form for you to fill in based on information obtained during the pre-installation conference call | ✓ | |
| Check your internal and external networks by referencing your network diagrams, and document any key items such as routers, servers, network protocols, and IP addresses etc | ✓ | |
| Check your hardware order to ensure you have all the proper components and configurations, including noting any hardware requirements such as mirrored drives and external devices | ✓ | |
| Order equipment (if needed) | ✓ | |
| Upon request provide the required policy and network information to us within the deployment form (if needed) | | ✓ |
| Provide the required Site to Site VPN tunnelling configuration | | ✓ |
| Provide the required Client to Site VPN tunnelling configuration | | ✓ |
| Provide the required security and outage contact information within the deployment form | | ✓ |
| Provide the required critical asset information for your network and servers | | ✓ |
| Collect and compiling any remaining installation information that may be required into the deployment form from you | ✓ | |

| | | |
|---|---|---|
| Configure shared infrastructure, including VPN tunnel to receive your logs (and your security events if needed) | ✓ | |
| Apply the default correlation policy to your security events if applicable | ✓ | |
| Test basic functionality and connectivity to your device | ✓ | |
| Configure the policy, if applicable test for functionality and connectivity | | |
| Provide detailed information to Telstra for the formal test plan to test functionality and connectivity to your security device to ensure we are receiving your log data (and your security events if needed) | | ✓ |
| Execute formal test plan in conjuction with you to test functionality and connectivity to your applications for final sign off | ✓ | ✓ |
| Prepare for transfer from the deployment team to MSS Operations team | ✓ | ✓ |
| Introduce our customer security portal website | ✓ | |
| Formally transferr support to the MSS Operations team and host a transition call with you and your team | ✓ | |
| Approve the detailed design and security policy that will be applied to your device | | ✓ |
| Test your equipment (power up and down) | ✓ | |
| Build your managed security service(s) platform (including hardware, software, and licenses) | ✓ | |

## 4. SERVICE ACTIVATION RESPONSIBILTIES

Various service activations and modification all have different responsibilities depending on the complexity of the action required. These responsibilities are listed below within the table.

4.1 The following service activation responsibilities apply to:

**Security Intelligence**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Provide login and password details if transferring device management to Telstra | | ✓ |
| Configure and install the security hardware and software to the relevant specifications as per Telstra security design once approved by you | ✓ | |
| Provide critical assets information to assist with the security event classification | | ✓ |

4.2 The following service activation responsibilities apply to**:**

**Managed Next Generation Firewall bundle**
**Managed Firewall**
**Managed IPS**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Provide login and password details if transferring device management to Telstra | | ✓ |
| Configure and install the security hardware and software to the relevant specifications as per Telstra security design once approved by you | ✓ | |
| Provide critical assets information to assist with the security event classification | | ✓ |
| Install and configure VPN client software on your end devices as required (if needed) | | ✓ |

# 5. DELOYMENT – ASSURANCE

Once your MSS solution has been installed and commissioned, the ongoing support will be transferred to the MSS Operations team, whose help desk will provide round-the-clock support for you.

Telstra has highly trained security experts on-site and available 24 hours a day, 7 days a week, 365 days a year, and they are reachable through the Telstra Security Services portal. This team will work diligently to resolve issues that may arise at any time.

## Accessing Customer Support

If there is an issue or question related to your MSS solution, the authorised contact from your organization can contact the MSS Operations team for support. The team is accessible online. To contact them, follow the steps below.

1. Login to the Telstra Security Services portal (described below) using a web browser and make a request for a change or report a problem.
   Web: https://security.telstra.com/mssportal
2. Type in the username and token credentials we supply to you.
3. Click the 'sign in' button.

## Quick Overview of the Security Portal

The Telstra Security Services portal provides a secure web connection over the Internet to the MSS Operations team. The Portal enables real-time access to a range of security resources, including:

- Detailed reports, including firewall and intrusion protection statistics and graphs.
- custom query capabilities.
- trouble ticket submission.
- security policy change requests.

## Quick Overview of the Policy Change Request

All policy change requests are placed through the security portal and will be placed directly into the MSS Operations team ticketing system and you will be given a ticket number that has been assigned to your request. You will be notified that the request has been received in accordance with your service level that you have purchased.

After acknowledging a change request, your policy change will be assigned to an analyst for validation and implementation. If there are any problems with the policy change request, or additional information is required for implementation, we will contact you.

Once the policy change request has been validated, it will be queued for implementation. All change request implementations will be attempted according to the service targets that apply to the service tier you have purchased.

Upon completing your policy changes, but prior to implementation, an analyst will validate the change to ensure to an error free implementation when validation is successfully completed. The change will be applied to your security device and you will be notified via the Telstra Security Services portal.

## 6. SERVICE TARGETS

The various targets for service activations and modifications all have different corresponding timelines depending on the complexity of the action required.

These timelines can also be affected by factors such as volume. For example, creating a simple policy rule on single appliance is a relatively minor piece of work, while creating complex policy rule across multiple security appliances can take an additional amount of time.

6.1 The following service targets apply to:

**Security Intelligence**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| **SERVICE MODIFICATIONS** | | |
| MINOR | | |
| Request to reset a password<br>Request to have user created<br>Change a Security Contact | ✓ | |
| MAJOR | | |
| Cancel a service<br>Relocate a service from one physical location to another location<br>Upgrade or downgrade from one management tier to another management tier | ✓ | |

6.2 The following service targets apply to:

**Managed Next Generation Firewall Bundle**
**Managed Firewall**
**Managed IPS**

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| **SERVICE MODIFICATIONS** | | |
| MINOR | | |
| Request to reset a password<br>Request to have user created<br>Change a Security Contact<br>Simple Policy Change<br>Simple Emergency Change | ✓ | |

| MAJOR | |
|---|---|
| Cancel a service | |
| Relocate a service from one physical location to another location | ✓ |
| Upgrade or downgrade from one management tier to another management tier | |
| Complex Policy Change | |
| Project Based Policy Change | |

## 7. GENERAL SERVICE RESPONSIBILTIES

Various service activations and modification all have different responsibilities depending on the complexity of the action required. These responsibilities for the MSS solution are listed below within the table.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Create additional user login accounts for end-users on the customer security portal | ✓ | ✓ |
| Managed login accounts for end-users on the customer security portal | | ✓ |
| Access and customized reports via the Telstra Security Services portal. For example real time log and security event data, device policy, threat Intelligent and assurance tickets | | ✓ |
| Advise Telstra of any changes to your product contact notifications for security events. | | ✓ |
| Specify any network changes that may affect the device operational (if you own and manage the network yourself) | | ✓ |
| Store your log data in secure manner and allow you to access this information via the Telstra Security Services portal if a request is made by you to us. | ✓ | |
| Store your event data in secure manner and allow you to access this information via the Telstra Security Services portal if a request is made by you to us. | ✓ | |
| Provide critical server asset information to assist us with your security event classification. | | ✓ |
| Contact the Telstra Helpdesk should you require your security PIN to be reset by us. | | ✓ |
| Contact the Telstra Helpdesk should you require a lost or faulty Token to be replaced by us | | ✓ |

## 8. SECURITY MONITORING RESPONSIBILITIES

Security Monitoring specific responsibilities are listed below in the table below.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| SERVICE ACTIVATION | | |
| Create and configure any accounts or platform changes required for connectivity and log extraction. You must configure your log sources to generate the appropriate log data and send the log data to the target collector. | | ✓ |
| Provide the means to capture the requirements ("Detailing workbook") to configure this product at initial setup. | ✓ | |
| Provide the requirements ("Detailing workbook") to configure this product at initial setup. | | ✓ |
| Ensure that Telstra is appropriately authorised to make agreed changes in response to Incidents that we have agreed to action on your behalf. This authorisation includes ensuring Telstra has appropriate access to your systems, personnel and resources. | | ✓ |
| Ensure your log generating system and data is fully compatible with the Security Monitoring service, including by ensuring that your system:<br>• is healthy, in a good condition, free of errors, with appropriate system patching and versions implemented; and<br>• has all necessary steps taken to reduce false positive alerts, and that the alerts you are seeing are real, actionable and provide relevant information. | | ✓ |
| ONGOING | | |
| To optomise your Security Monitoring service, we will tune that service. You must be available to facilitate that tuning for 40 calendar days, starting from the date we ask. | | ✓ |
| If you intend to make any changes to the physical infrastructure or to devices generating log data, you must obtain our prior written consent. | | ✓ |
| Provide you with service reporting data | ✓ | |

## 9. SECURITY INTELLIGENCE RESPONSIBILITIES

Security Intelligence specific responsibilities are listed below in the table below.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| Inform you of security events based on security event classification. | ✓ | |

## 10. MANAGED NEXT GENERATION FIREWALL BUNDLE RESPONSIBILITIES

Managed Next Generation Firewall bundle specific responsibilities are listed below in the table below.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| **MANAGED NEXT GENERATION FIREWALL** | | |
| Undertake acceptance testing of the device configuration. | ✓ | ✓ |
| Log any configuration or policy changes within the Telstra Security Services portal (simple, complex and/or emergency changes) | | ✓ |
| Specify settings, such as ports, filters, traffic direction, rules and network address translations for the firewall policy. | | ✓ |
| Specify VPN tunnels - site to site IPSEC and client to site IPSEC/SSL specifications | | ✓ |
| Administer changes to the firewall that have been submitted via the Telstra Security Services portal based on the service tier you have purchased | ✓ | |
| Apply version control to the policy and store up to 7 previous versions | ✓ | |
| Backup the specified firewall and IPS settings and restore settings in the event of a failure | ✓ | |
| Inform you of security events based on security event classification. | ✓ | |
| Renew equipment maintenance | ✓ | |
| Maintain device asset information within Telstra systems and customer portal | ✓ | |
| Replace faulty equipment based on the service tier that has been purchased by you (provided you have transferred this reasonability to Telstra) | ✓ | |
| Apply content and signature updates to (UTM firewall features) based on the service tier that you have purchased | ✓ | |
| Analyse and install selected minor security fixes and operating system hot fixes applicable to your device | ✓ | |
| Provide device health and availability (outage) alarms based on the service tier you have purchased | ✓ | |
| Log and manage external support cases to vendors | ✓ | |
| Advise Telstra of any changes to your product contact notifications for outage and maintenance requests | | ✓ |

## 11. MANAGED FIREWALL RESPONSIBILITIES

Managed Firewall specific responsibilities are listed below in the table below.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| **MANAGED FIREWALL** | | |
| Undertake acceptance testing of the device configuration. | ✓ | ✓ |
| Log any configuration or policy changes within the Telstra Security Services portal (simple, complex and/or emergency changes) | | ✓ |
| Specify settings, such as ports, filters, traffic direction, rules and network address translations for the firewall policy. | | ✓ |
| Specify VPN tunnels - site to site IPSEC and client to site IPSEC/SSL specifications | | ✓ |
| Administer changes to the firewall that have been submitted via the Telstra Security Services portal based on the service tier you have purchased | ✓ | |
| Apply version control to the policy and store up to 7 previous versions | ✓ | |
| Backup the specified firewall settings and restore settings in the event of a failure | ✓ | |
| Inform you of security events based on security event classification. | ✓ | |
| Renew equipment maintenance (provided you have transferred this reasonability to Telstra) | ✓ | |
| Maintain assets information within Telstra systems and customer portal | ✓ | |
| Replace faulty equipment based on the service tier that has been purchased by you (provided you have transferred this reasonability to Telstra) | ✓ | |
| Apply content and signature updates to (UTM firewall features) based on the service tier that you have purchased | ✓ | |
| Analyse and install selected minor security fixes and operating system hot fixes applicable to your device | ✓ | |
| Provide device health and availability (outage) alarms based on the service tier you have purchased | ✓ | |
| Log and manage external support cases to vendors | ✓ | |
| Advise Telstra of any changes to your product contact notifications for outage and maintenance requests | | ✓ |

## 12. MANAGED INTRUSION PROTECTION SERVICE RESPONSIBILITIES

Managed IPS specific responsibilities are listed below in the table below.

| REQUIREMENT | RESPONSIBILITY | |
|---|---|---|
| | US | YOU |
| **MANAGED NETWORK INTRUSION PROTECTION** | | |
| Undertake acceptance testing of the device configuration | ✓ | ✓ |
| Log any configuration or policy changes within the Telstra Security Services portal (simple, complex and or emergency changes) | | ✓ |
| Specify settings, such as disabling and enabling event information, specifying event information for Security Severity Definitions | | ✓ |
| Administer changes that have submitted via the customer portal based on the service tier you have purchased | ✓ | |
| Apply version control to the policy and store up to 7 previous versions | ✓ | |
| Backup the specified IPS settings and restore settings in the event of a failure | ✓ | |
| Inform you of security events based on security event classification. | ✓ | |
| Renew equipment maintenance (provide you have transfer this reasonability to Telstra) | ✓ | |
| Replace faulty equipment based on the service tier that has been purchased by you (provided you have transferred this reasonability to Telstra) | ✓ | |
| Apply content and signature updates to the devices based on the service tier that you have purchased | ✓ | |
| Analyse and install selected minor security fixes and operating system hot fixes applicable to your device | ✓ | |
| Provide device health and availability (outage) alarms based on the service tier you have purchased | ✓ | |
| Managed and log external support cases to vendors | ✓ | |
| Advise Telstra of any changes to your product contact notifications for outage and maintenance requests | | ✓ |