DDoS Attack Mitigation Service Specific Terms and Conditions

The Sure DDoS Attack Mitigation Service provides the Customer with a solution to help protect the Customer site against Distributed Denial of Service (DDoS) attacks by analysing incoming traffic, detecting attack conditions and blocking the malicious traffic whilst letting genuine traffic through.

DDoS ATTACK MITIGATION SERVICE SPECIFIC TERMS AND CONDITIONS

The Sure DDoS Attack Mitigation Service Specific Terms and Conditions should be read in conjunction with the Customers Master Services Agreement or Sure General Terms and Conditions (as applicable), and the Order Form. In the event of a conflict the DDoS Attack Mitigation Service Specific Terms and Conditions and relevant Order Form will take precedence over the Customers Master Services Agreement or Sure General Terms and Conditions (as applicable). Where we refer to the "Agreement" in these DDoS Attack Mitigation Service Specific Terms and Conditions, we mean these terms and conditions, the Sure General Terms and Conditions and your Order Form. The Agreement constitutes a legally binding agreement between you and us.

In these DDoS Attack Mitigation Service Specific Terms and Conditions "we", "us" or "our" means Foreshore Limited, Sure (Guernsey) Limited, Sure (Jersey) Limited or Sure (Isle of Man) Limited (as applicable and as specified on the applicable Order Form) and "you" or "your" means the customer named on the Order.

These DDoS Attack Mitigation Service Specific Terms and Conditions supersede and replace all previous versions.

1. Definitions and Interpretation

The definitions provided in this section (Definitions and Interpretation), exist in addition to those definitions outlined in the Sure General Terms and Conditions and any undefined terms have the meaning given to those terms in the General Terms and Conditions.

"Alert" means a Misuse Detection that has exceeded the configured threshold. Misuse Detections will initiate automatic mitigation, except where configured not to. The Customer can access information on Detections in the Sure Portal and can receive automated Alert emails.

"**Alert Information**" means information provided to the Customer by the Sure Portal.

"Approved Personnel" means those Customer personnel listed during the on boarding process that may request changes to the DDoS Attack Mitigation Service.

"Attack" or "Attack Incident" means an event in which malicious traffic (e.g. "DDoS"), is directed at an endpoint which is protected by Sure Attack Mitigation Devices. The determination as to whether traffic is Attack traffic shall be determined solely by Sure.

"Attack Mitigation using Sure Attack Mitigation Devices" means the mitigation of a DDoS attack using Sure Attack Mitigation Devices. After detection of a suspected DDoS attack, mitigation can be initialised in the Sure Attack Mitigation Devices. The Sure Attack Mitigation Devices are able to filter traffic within the Sure network and allows for a minimum of a single/32 address to be redirected. Filtered traffic is returned to the core network after cleaning to complete its journey.

"Baseline" The traffic rate that the Sure Attack Mitigation Devices expects given a predefined configuration that the Sure Attack Mitigation Devices typically expect on each router.

"Black Holing" means discarding all data destined for a particular IP Address to prevent the disruption, and or flow of, data destined for other IP Addresses.

"Business Day" means a day, from 08-00 to 17-00 hours Monday through Friday that is considered a normal working day in Guernsey, Jersey and the Isle of Man and shall exclude all bank and public holidays in Guernsey, Jersey or the Isle of Man.

"Configuration" means -the configuration of a sub-division of the equipment or services monitored by the DDoS Attack Mitigation Service which contains IP Addresses for a group of protected servers and equipment. The DDoS Attack Mitigation Service provides protection for those IP Addresses only.

"Critical Change" means a change required by the Customer or the Sure SOC, without which there will be a serious business impact on the Customers online operation, but also includes the serious business impact to any Sure Customer if such a change were not made. Critical change shall also mean anything that is likely to affect the Customer's traffic via the protected network including but not limited to architectural changes, e.g. new internet application, change in bandwidth, new servers, new IP addresses, changes in infrastructure and any change in Customer activity that might reasonably change the Customers traffic profile.

"Denial of Service (DoS)" means an Attack that is an attempt by an attacker to exhaust the resources available to a network, application, or service so that genuine users cannot gain access. The majority of attacks are commonly referred to as Distributed DoS attacks (DDoS), Such attacks are DoS attacks launched from multiple different hosts simultaneously; and, in the case of a botnet, could be 10s, 100s or 1,000s of machines globally distributed.

"Distributed Denial of Service (DDoS)" means Attacks that will generally fall into one of three broad categories:

Volumetric Attacks: Attempts to consume bandwidth either within a target network or service or between a target network or service and the Internet. Such attacks are aimed at causing network congestion.

TCP State-Exhaustion Attacks: Attempts to consume connection state tables present in many infrastructure components such as load-balancers, firewalls and application servers. Even high-capacity devices capable of maintaining state on millions of connections can be impacted by such attacks.

Application Layer Attacks: Target some aspect of an application or service at Layer-7. Such attacks can be very effective and can be triggered using as few as one attacking machine generating a low traffic rate.

"**DDoS Attack Mitigation Service (Mitigation)**" means the platform(s) and services that provide and comprises the management and operation of a mitigation solution offered by Sure to the Customer. The DDoS Attack Mitigation Service provides on-net Attack Mitigation using Sure Attack Mitigation Devices. The DDoS Attack Mitigation Service is managed and operated by Sure. In summary the DDoS Attack Mitigation Service includes analysing incoming traffic destined for a pre-defined set of IP addresses, detecting suspected attack conditions, filtering affected traffic, and discarding malicious packets whilst retaining the genuine traffic.

"Event Log" means a log file where an Operating System or a Hosted Application stores information about events for future analysis. Log files can be generated by equipment used in the provision of the DDoS Attack Mitigation Service.

"Hosted Application" means a World Wide Web or other application hosted upon Customer or Sure Equipment containing World Wide Web, Internet or intranet content.

"Hosting Solution" means a collection of services taken as a single solution provided by Sure to the Customer.

“**Incident Response**” means the response by the SOC to an alert raised by the monitoring of the Service.

“**Incident Response Procedure**” means the procedure to respond to an incident outlined in the Provision of Service section of the DDoS Attack Mitigation Service Specific Terms and Conditions.

“IP Address” means the identifying number of a device attached to the Internet. Every device which connects to the Internet must have a unique IP Address. IP Addresses are written as four sets of numbers separated by full stops: for example 204.171.64.2.

“Misuse Detection” means the detection of excessive rates of traffic flowing inbound on any of Sure’s Internet edge interfaces that is directed toward individual hosts within a Configuration in the service. Sure Attack Mitigation Devices detect misuse attacks by comparing traffic to misuse signatures and rate thresholds. When Sure Attack Mitigation Devices detect a misuse attack, it gathers details about the attack traffic on the affected routers. The Misuse Detection is applied on a per Configuration basis.

“Service Operation Centre (SOC)”, operated by Sure as a service management centre, is one or more locations from which network monitoring, control, or management, is exercised. The SOC provides a 24x365 service and a single point of contact to the Customer.

“Operating System” means a computer programme installed on a server, which enables the Customer’s software and Hosted Applications to run on that server.

“**Order Form**” means the Sure Order Form, signed by the Customer, detailing the DDoS Attach Mitigation Service ordered and other relevant information forming part of this Agreement.

“**Professional Services**” means the provision of security consulting services chargeable at an hourly rate as specified on the Order Form.

“**Sure**” means either Foreshore Limited, Sure (Guernsey) Limited, Sure (Jersey) Limited or Sure (Isle of Man) Limited as stated in the relevant Order Form.

“**Sure Attack Mitigation Devices**” means network appliances to provide network wide intelligence, anomaly detection, threat management, and traffic-scrubbing owned and managed by Sure.

“Sure Portal” means a website hosted by Sure providing an interface into the DDOS Attack Mitigation Service. The Portal provides the Customer with information for their DDoS Attack Mitigation Service.

2. Provision of the Service

2.1. The DDoS Attack Mitigation Service consists of the following:

2.1.1 Configuration and maintenance of the DDoS Attack Mitigation Service on the relevant equipment owned and managed by Sure.

2.1.2 Configuration of a set of pre-defined monitoring parameters as indicated on the Order Form, and as agreed between the parties during the on-board process.

2.1.3 A DDoS information facility via the Sure Portal.

2.1.4 The on boarding process will specify Customer’s authorised contact personnel and portal administrator for use when configuration changes are required, or in the event of an attack. If the Customer’s Hosting Solution includes appropriate Operating System or Hosted Application management services, Sure can be directed to use the same contacts.

2.1.5. The Sure Incident Response Process must be used by the Customer to request any subsequent changes to their Configuration, to define DDoS Contact Personnel in 2.1.4 and the DDoS Attack Mitigation Service to be provided to the Customer. Sure may request the Customer to update the information held regarding this service from time to time.

2.1.6 In the event that Sure Attack Mitigation Devices detect an alert, the relevant Incident Response Procedure will be followed.

2.1.7. The Sure DDoS Attack Mitigation Service can detect and alert, on the following

- **Misuse attacks against specific web servers** – Internet Control Message Protocol (ICMP), Transmission Core Protocol (TCP) NUL, TCP SYN, TCP RST, IP NULL, IP Fragment, IP private address space and Domain Name System (DNS) flood attacks.
- **Traffic anomalies** – including high-bandwidth threats like User Datagram Protocol (UDP) floods.
- **Application attacks** – including repeated Hypertext Transfer Protocol (HTTP) GET website commands, DNS flood attacks on DNS servers and malformed DNS requests.

2.2 **Monitoring and Detection** consists of the following:

2.2.1 The monitoring and detection of Alerts as part of the DDoS Attack Mitigation Service provides a set level of passive monitoring of incoming traffic against the Customer's protected Configuration, to build a Baseline or profile of normal traffic patterns and behaviour.

2.2.2 With Misuse Detection traffic flows are constantly monitored and compared to predefined rules and rate thresholds. If any of these are exceeded the Sure DDoS Attack Mitigation Devices will identify the target by its IP Address and generate an alert. Automated Alert emails will be sent to the Customers DDoS Personnel, and Alerts will initiate mitigation automatically. Customers may access the Sure Portal for real time and historic information on traffic flows, alerts and mitigations.

2.3 Cleaning and Mitigation consists of the following:

2.3.1 The Cleaning and Mitigation of an Attack occurs following the Monitoring and Detection of an Alert and when a mitigation is initiated automatically. Traffic destined for the targeted IP Address(es), will be inspected by Sure DDoS Attack Mitigation Devices. Such traffic will be subjected to multiple layers of statistical analysis, active verification and anomaly recognition to identify malicious sources, reveal abnormal behaviour and to discard suspected packets that do not conform to the normal traffic pattern.

3.0 Incident Response Procedures consist of the following:

3.1 Proactive monitoring of will be undertaken by Sure Attack Mitigation Devices and Customer generated service incidents in this section will be undertaken by the SOC. The reactive notification of DDoS attacks can also be undertaken by the Customer. In the event of a Customer suspecting they are suffering from a DDoS attack, that has not been identified by the Sure Attack Mitigation Devices, the Customer should contact the SOC and advise them of this. The SOC will investigate and will follow the appropriate Incident Response procedures.

3.2 The Misuse Detection Alert incident response procedure consists of the following;

A Misuse Detection Alert is generated following the triggering of the predefined rules and anomalous traffic being directed toward an individual host IP Address(es) within the Configuration. The Sure Attack Mitigation Devices detect misuse attacks by comparing traffic entering Sure internet edge router interfaces predefined rules and rate thresholds. When the Sure Attack Mitigation Devices detect a misuse attack, it gathers and records details about the attack traffic on the affected router interfaces.

Sure will configure the Attack Mitigation Devices predefine rules and thresholds. This process is designed to ensure immediate mitigation actions are taken as soon as the rules are triggered.

3.2.1 Misuse Detection Alert process

Step	Owner	Action	Timeline
Ongoing	SOC	SOC monitor service on a 24 x 7 basis	Ongoing
Step 1 Misuse Detection Alert condition detected	SOC	An automated email is sent to the Customer DDoS Personnel email address(es) containing a reference to the Alert on the Sure Portal. The Customer may access the Sure Portal Alert details as required	On detection of Misuse Detection Alert
Step 2 Initiation of automated DDoS mitigation using Sure Attack Mitigation devices	SOC	I. Automatic mitigation is triggered using the Sure Attack Mitigation Devices. The mitigation will use the mitigation predefined rules II. Anautomated email is sent to Customer DDoS Personnel email address (es), it will Advise that an automatic mitigation has commenced and will contain a reference to the Alert on the Sure Portal III. The Customer may access the Sure Portal and view the mitigation in progress	On detection of Misuse Detection Alert
Step 3 Monitoring and diagnostics during a mitigation	SOC & Customer	I. The SOC will continue to monitor the mitigation II. IP Engineering may need to manually support the Customer with changes to the Configuration as part of the ongoing mitigation process. III. The Customer may call the SOC to review status, discuss progress and request updates **2nd & 3rd Line Involvement** The SOC may escalate to second and third level expertise within, and external to, Sure as required during a mitigation for assistance	Ongoing for the duration of the mitigation
Misuse Detection - Incident Resolution and Closure - Using Sure Attack Mitigation Devices			
Step 4 Incident Resolution & closure	SOC	Where a single mitigation was automated using Sure Attack Mitigation Devices, the mitigation will complete automatically once the Alert has ended.	As advised by the SOC and agreed by all Parties.

Step 5 Misuse Detection Alert condition ended and Mitigation Ended	SOC	I. An automated email is sent to the Customer email address(es) to advise that the Alert has now ended, and the automatic or manual mitigation has stopped with a reference to the alert in the Sure Portal to allow customer to access alert details if required. II. Customers can review information on all historical mitigations within the Sure Portal	**For Automatic Mitigations** Occurs on completion of an automatic mitigation event **For Manual Mitigations** Will be manually stopped by the SOC

3.3 Sure will use reasonable endeavours to ensure that legitimate traffic is received as normally as possible during any attack, and that the configured IP Address (es) are affected as little as possible. During an attack, countermeasures will be deployed by Sure to ensure disruptions to operations are minimised, and measures such as "Black Holing" will only be used by Sure if Sure deems its network or other customer services to be at risk.

3.4 During any Distributed Denial of Service attack Sure will work with the Customer, where required, to fine tune the DDoS Attack Mitigation Service to achieve the maximum DDoS protection available with the minimum processing overhead and traffic disruption.

3.5 During the calendar month and immediately following the Service Delivery Date, Sure will allow what it considers reasonable changes to the Configuration to be covered by the initial connection charge. Thereafter, Sure will perform a maximum of one Critical Change to the Configuration of the DDoS Attack Mitigation Service or the Customer Configuration in any calendar month. Further changes requested by the Customers DDoS Personnel will be charged according to the rates on the Order From.

3.6 Services **not included** – The Sure DDoS Attack Mitigation Service neither offers nor provides:

- Permanent archival and storage of log files
- Forensics and investigations
- Legal case preparation, PR incident support
- Security consulting services (e.g. security policy design, security auditing, penetration testing, contingency or disaster recovery planning, etc.)
- Security reporting and analysis
- Permanent filtering or cleaning of traffic

3.7 The Customer will not have access to any DDoS Attack Mitigation Service equipment or software as part of this service, except for access to the Sure Portal.

4. Service Management

This section refers to the service management of the DDoS Attack Mitigation Services using Sure Attack Mitigation Devices in preparation for, during and post DDoS attacks. Service management support includes providing a single point of contact for the preparation and coordination of the following:

- Preparation and ongoing maintenance of the Customer associated Configuration
- Non urgent configuration changes requested by the Customer
- Telephone support for Customer service reviews
- 24x365 Operational support for DDoS Alerts and escalations

- Investigating issues of Sure Portal availability for the Customer

4.1 Management Information

Customer traffic, alerts, and mitigation information shall be available on the Sure Portal.

4.2 Quarterly Reviews

Quarterly Reviews will be carried out, at the Customer's request, between Sure and the Customers Approved Personnel.

4.3 Major Incident Report

Following a service affecting DDoS incident, reports are produced at the request of the Customers Approved Personnel.

4.4 Escalation

Sure will strive to achieve a resolution for our Customers within their contracted Service Levels. However, we understand that there may be times when our Customers wish to escalate an ongoing incident, and for this purpose only the SOC has a 5-level escalation process.

It is recommended that the Customer involve the Sure SOC in all escalations although the Customer is entitled to escalate directly to the persons listed below. The SOC's contact details are as follows:

Tel: **+44 (0) 1534 752310**
Email: **serviceoperations@sure.com**

To initiate an escalation, please either call the SOC and ask to escalate to the appropriate level or call the number in the table below. Please use the escalation management information to determine the appropriate level and contact, noting that the minimum time must have first elapsed. Only contacts registered with Sure are permitted to escalate, for security reasons.

Level	Position	Telephone Number
Level 1	Service Operation Centre (SOC) - Front Desk	+44 (0) 1534 752310
Level 2	Service Operation Centre (SOC) – Senior Support Technician	+44 (0) 1534 752310
Level 3	Duty Operations Manager	+44 (0) 7700 722407
Level 4	Head of Service Assurance	+44 (0) 7700 722408
Level 5	CTIO	+44 (0) 7700 722409

** Or such other person as is notified to the other Party. If there is any change in the contact details of those listed above, each Party shall immediately notify the other in writing.*

4.5 Engineering configuration changes

Charges for engineering configuration changes will be made when we are requested to add new monitored IP address configurations to an existing Sure DDoS Attack Mitigation Service. There will be no Charge for removing redundant configuration elements. Requests for additional engineering configuration changes outside the scope of the DDoS Attack Mitigation Service can also be provided and are quoted for at the hourly rates detailed on the Order Form or on request from Sure.

5.0 Maintenance

5.1 Emergency Maintenance

Emergency Maintenance may be required by Sure for instances that if left unattended, already have or could imminently result in an outage or the significant degradation of the DDoS Attack Mitigation Service, Sure networks and/or IP bandwidth services delivered to other customers.

When considering Emergency Maintenance Sure will endeavour where possible to give the Customers DDoS Personnel 24 hours' notice for items listed below:

- Critical Security Updates
- Critical IOS/Software updates
- Equipment failure and replacement

5.2 Normal Maintenance/Upgrades

Sure may periodically need to maintain or upgrade the DDOS Attack Mitigation Service to ensure the latest software and hardware versions are in operation. If Sure determines, in Sure's sole discretion, that an upgrade is necessary, Sure will work with the Customers DDoS Personnel to schedule a time to make the necessary changes. The Customers DDoS Personnel must allow Sure to make these changes within five Business Days of receipt of the notification from Sure to do so. If the Customers DDoS Personnel does not respond to a Sure notification to undertake the maintenance, Sure will make the change at a time Sure considers to be most convenient for all Parties.

6. The Sure Portal

The Sure Portal provides the Customer with access to various information including but not limited to Alerts and Attack Mitigations using Sure Attack Mitigation Devices.

6.1 The following information is provided as part of the DDoS Attack Mitigation Service and is available for the Customer to access at the Sure Portal:

> 6.1.1 Counters and graphs provide a high–level overview of the Customer's protected Configuration, showing current Alerts, Attacks and incoming and outgoing traffic to aid Customer's ability to determine the current status of their Service.
>
> 6.1.2 Historical information provides a visual record of Attacks and associated Alert responses for determining Attack patterns and allowing verification of successful protection against Attacks.

7. Liability

7.1 Clause 26 (Liability) of the General Terms and Conditions apply and Sure will not be liable for incidental, indirect, exemplary, or consequential damages of any kind, including, but not limited to, damage caused to the Customer due to the operation of the DDoS Attack Mitigation Service or damages related to lost data or lost profits, even if Sure have been advised of the possibility of such damages.

7.2 This service is designed to protect the Customer and the Customer's end users from DDoS attacks. However, Sure do not warrant that it shall withstand these attacks on all occasions. Sure reserve the right to "Black Hole" any of the Customer's traffic as required to protect the Sure network and other customers.

8. Charges

The following categories of charges apply to the DDoS Attack Mitigation Service:

CATEGORY OF CHARGE	NATURE OF CHARGE
Installation, configuration, and protection using the Sure DDoS Attack Mitigation Service using Sure Attack Mitigation Devices (depending on amount of bandwidth protected or number protected IP addresses)	Non-Recurring Charge plus Monthly Recurring Charge
Make critical change	Non-Recurring Charge
Engineering configuration changes	Non-Recurring Charge

The actual charges are shown on the relevant Order Form, which is available on request from Sure (Guernsey) Limited, PO Box 3, Centenary House, La Vrangue, St Peter Port, Guernsey, GY1 2EY, or by calling Sales on 01481 700700.

9. Payment

9.1 The Customer shall pay to Sure on demand all applicable charges for the relevant Service at rates which are available on request from Sure at the above address.

9.2 Rental for the Service will start on the Service Delivery Date, unless:

9.2.1 Sure notify the Customer of a later date for the start of Service when rental will be payable from; or

9.2.2 The Customer uses the Service before the Service Delivery Date; in which case rental will be payable from the date the Customer first uses the Service.

9.3 Rental is normally payable in advance but Sure may bill the Customer in arrears. Except for temporary Service, the Customer must pay rental in accordance with the Sure billing cycle. Sure will apportion rental on a daily basis for incomplete billing periods.

10. Service Schedule and Service Level Agreement

The DDoS Attack Mitigation Service provides the following operational SLAs:

Name	Description	Target
Standard Hours of Cover	Sure undertake to provide service to the Customer	24 x 365
DDoS Service Availability monitoring	The availability of Sure Attack Mitigation Devices	99.9%
DDoS Attack notification	Automated email Alerts will be notified to the customer by the Sure Portal	Automatic upon detection
Time to mitigation using Sure Attack Mitigation Devices with automatic mitigation	The time to mitigation from Misuse Detection Alert where automatic mitigation is configured.	Automatic upon detection

Time to mitigation using Sure Attack Mitigation Devices with manual mitigation	The time to mitigation from Misuse Detection Alert where automatic mitigation is not configured, or from a Customer requested manual mitigation	30 minutes from mitigation approval from the Customer

11. The DDoS Attack Mitigation Service provides the following provisioning or change request SLAs:

Provision of Service	Install within 6 working days of receipt of information required in the Provision of Service section above.
Critical Change	Response: Within 1 hour Resolution: Within 4 hours

If the Customer requests Sure responds and works on a Critical Change and that Critical Change is subsequently found not to be a Critical Change then Sure reserve the right to make a charge based on the engineer applicable rate per hour.

Sure will provide the Customer with the Service on the terms and conditions as stated.

Sure plan to deliver a working service by the time agreed with the Customer or within the maximum time for provision of the Service as stated on the Order Form.

Requests made to Sure relating to the provision of the Service must be made by email to the Customers assigned Sure Account Manager and or Sure Service Manager.

Notwithstanding and without limiting the generality of the Sure General Terms and Conditions, Sure will not be liable for any failure to meet the standard provision target times or level of Fault response caused by matters beyond Sure’s reasonable control.

If the Customer requires any work for the provision of service to be undertaken outside of Normal Working Hours then a charge will be made based on the applicable hourly engineering rate.

12. Fault Support for the DDoS Attack Mitigation Service

Fault Support	Is provided via the SOC on the contact numbers provided
Fault cover	24 hours per day
Fault Response	Within 1 hour of receipt of Fault report
Fault clear	Resumption of service within 8 hours excluding where replacement hardware is required as in the Maintenance section above.

Where a resolution to the Customer's satisfaction cannot be made at the time of reporting a Fault then Sure will ask the Customer to provide Sure with a contact telephone number to enable reports on progress with the Fault clearance to be made.

Sure will:

1. Provide advice by telephone
2. Carry out tests and diagnostics on the Service
3. If required, visit the Customer's Premises or work to a point in the Sure network
4. Work to resolve the Fault within the agreed time period as stated in the table set out above

If Sure respond and work on a reported Fault and it is subsequently found not to be a Fault with Sure service then a charge will be made based on the applicable engineering rate.