# DDoS Attack Mitigation Service 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 TERMS AND CONDITIONS**

**The Sure DDoS Attack Mitigation Service 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 Terms and Conditions and relevant Order Form will take precedence over the Customers Master Services Agreement or Sure General Terms and Conditions (as applicable).**

**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.

**"Alerts"** means Alert types as referred to by this service description as Automated Email, High, Medium or Low.

**"Cloud Partner Facilities"** Means a global network of on-demand cloud-based scrubbing centres, Security Operations Centre (SOC) and the on-demand cloud-based service which "cleans" or "scrubs" certain internet-based malicious, attack traffic from a stream of internet based traffic directed at the Customer's endpoint.

"**Alert Reports**" means reports provided to the Customer by the Sure Portal.

**"Approved Personnel"** means those Customer personnel listed in the On Boarding Document 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 either by Sure Attack Mitigation Devices or Cloud Partner Facilities. The determination as to whether traffic is Attack traffic shall be determined solely by Sure and its Cloud Partner Facilities operator.

**"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 by directing traffic to 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.

**"Attack Mitigation using Cloud Partner Facilities"** means the mitigation of a DDoS attack using Cloud Partner Facilities. After detection of a suspected DDoS attack, upon agreement by all parties, mitigation can be initialised by re-routing traffic to the Cloud Partner Facilities. Cloud Partner Facilities will only be used for volumetric attacks that exceed the capacity of the Sure Attack Mitigation Devices. The Cloud Partner Facilities will use various mitigation techniques and allows for a minimum of a single/24 subnet to be redirected. Filtered traffic is returned from Cloud Partner Facilities to the Sure network after cleaning to complete its journey. The diversion of traffic to Cloud Partner Facilities is subject to The Customers approval and will incur an additional Mitigation Incident Fee as listed on the service Order Form.

**"Baseline"** The traffic rate that the Sure Attack Mitigation Devices expects given a Managed Object configuration or the profiled traffic rate 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 and shall exclude all bank and public holidays in Guernsey.

**"Critical Change"** means a change required by the Customer or the NOC, 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 multi-layer, multivendor DDoS mitigation solution offered by Sure to the Customer. The DDoS Attack Mitigation Service provides on-net Attack Mitigation using Sure Attack Mitigation Devices and/or above-net Attack Mitigation using Cloud Partner Facilities. 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 Managed Objects, 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.

**"High Alert"** means a high severity Profiled Detection or Misuse Detection that has exceeded the configured or profiled threshold defined as high severity. High severity Misuse Detections will initiate automatic mitigation, except where configured not to. High severity Profiled Detections may initiate automatic mitigation where requested by the Customer. The Customer can access reports on high severity Detections in the Sure Portal and can receive automated High Alert emails.

**"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 NOC 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 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.

**"Low Alert"** means a Profiled Detection or Misuse Detection that has reached the configured or profiled thresholds defined as low severity. The Customer can access reports on Low Alerts in the Sure Portal and can receive automated Low Alert emails on request.

**"Managed Object"** means 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.

**"Medium Alert"** means a Profiled Detection or Misuse Detection alert that has reached a point between the configured or profiled thresholds defined as Low Alert and High Alert. The Customer can access reports on Medium Alerts in the Sure Portal and can receive automated Medium Alert emails on request.

**"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 configured Managed Object. 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 high severity rate for Misuse Detection is applied on a per Managed Object basis.

**"Mitigation Incident Fee"** shall mean the fee that applies to an Attack Mitigation using Cloud Partner Facilities. The Mitigation Incident Fee shall cover a period of up to seventy two (72) consecutive hours or any portion thereof. Attack Mitigation using Cloud Partner Facilities for longer than seventy two (72) consecutive hours are subject to Mitigation Incident Fees for each period of consecutive seventy two (72) hours or any part thereof.

**"Non-Critical Change"** is a change such as a request for a configuration which has no immediate or significant impact on the running of the Customer online operation.

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

**"On Boarding Document"** is the document to be completed by the Customer to provide information to allow Sure to provide the DDoS Attack Mitigation Service. It shall be agreed between all parties at the time of ordering, and shall be reviewed from time to time to verify the configuration that is applied to the DDoS Attack Mitigation Service. Any changes or additions to the configuration of the Service may require a new On Boarding Document or Order From to be completed as appropriate.

**"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 Attack 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.

**"Profiled Detection"** means identifying excessive rates of traffic for a Managed Object when compared to manually set thresholds or against the traffic rate that the Sure Attack Mitigation Device expects on each monitored router. The traffic rate that the Sure Attack Mitigation Devices expect is referred to as the Baseline. When the Attack Mitigation Devices detects a profiled anomaly, it gathers details about the anomalous traffic on the affected Managed Object and includes it in the Alert. Profiled Detection can generate false positives (for instance if a large file is transferred across a VPN) and so is provided as an optionally configured additional benefit to the Customer on request and the Customer may receive automatic email alerts or access reports in the Sure Portal.

**"Security Operation Centre (SOC)"** means the dedicated Security Operation Centre operated by Sure's Cloud Partner Facilities provider as part of the Cloud Partner Facilities service. The SOC provides a 24x365 service.

**"Sure"** means either 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 various reports for their DDoS Attack Mitigation Service. The portal will not display mitigation information when Attack Mitigation using Cloud Partner Facilities are in use.

**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 and also the pre-configuration of services that enable Attack Mitigation using Cloud Partner Facilities.

2.1.2 Configuration of a set of pre-defined monitoring parameters for each Managed Object(s) as indicated on the Order Form, and as agreed between the parties and defined within the relevant customer On Boarding Document. Within the On Boarding Document the Customer must specify the IP Addresses and IP Address ranges, applications and protocols that the Customer wishes the DDoS Attack Mitigation Service to be activated for (e.g. Machine 10.10.1 0.23, Web server, TCP port 80 (HTTP) and port 443 (HTTPS)).

2.1.3 A reporting facility via the Sure Portal.

2.1.4 The On Boarding Document will specify Customer's authorised contact personnel 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 On Boarding Document must also be completed by the Customer to request any subsequent changes to the Managed Objects, to define Approved 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 On Boarding Document from time to time.

2.1.6 In the event that Sure Attack Mitigation Devices detect a High 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.
- **Profile 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 Managed Object thresholds, to build a Baseline or profile of normal Customer traffic patterns and behaviour.

2.2.2 With Misuse Detection traffic flows are constantly monitored and compared to misuse signatures 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 alerts based on the calculated severity. Automated Alert emails will be sent to the Customers Approved Personnel, and High Alerts will initiate mitigation automatically where configured. Customers may access the Sure Portal for real time and historic information on traffic flows, alerts and mitigations.

2.2.3 With optional Profiled Detection, traffic flows can be constantly monitored and compared against the Baseline, looking for any deviations that might indicate a potential attack. If any abnormal or unusual behaviour is detected the Sure DDoS Attack Mitigation Devices will identify the target by its IP Address and generate alerts based on the calculated severity.

**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 either automatically or manually. Traffic destined for the targeted IP Address(es), will be redirected from the main path for inspection by Sure DDoS Attack Mitigation Devices. Diverted 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 service incidents in this section will be undertaken by the NOC and Sure Attack Mitigation Devices.

3.1.1 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 NOC and advise them of this. The NOC will investigate and will follow the appropriate Incident Response procedures.

3.1.2 Incident Response procedures are sub divided into Misuse Detection Alert procedures and optional Profile Detection Alert procedures.

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

A Misuse Detection Alert is generated following the detection of excessive rates of traffic being directed toward an individual host IP Address(es) within a Managed Object. The Sure Attack Mitigation Devices detect misuse attacks by comparing traffic entering Sure internet edge router interfaces to misuse signatures 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 Customer's Managed Object high severity thresholds as agreed with the Customer. This process is designed to ensure immediate mitigation actions are taken as soon as the Customer's high severity threshold is breached. This threshold will be defined in the On Boarding Document and may be modified at the request of the Customer.

**3.2.1 Misuse Detection Alert process**

| Step | Owner | Action | Timeline |
|---|---|---|---|
| Ongoing | NOC | NOC monitor service on a 24 x 7 basis | Ongoing |
| **Step 1** High severity Misuse Detection Alert condition detected | NOC | An automated email is sent to the Customer Approved Personnel email address(es) containing a hyperlink to the Alert on the Sure Portal. The Customer may access the Sure Portal Alert details as required | On detection of high severity Misuse Detection Alert |
| **Step 2** Initiation of automated DDoS mitigation using Sure Attack Mitigation devices | NOC | I. Automatic mitigation is triggered using the Sure Attack Mitigation Devices. The mitigation will use the mitigation template configured for the Customer<br>II. An automated email is sent to Customer Approved Personnel email address (es), it will advise that an automatic mitigation has commenced and will contain a hyperlink to the Alert on the Sure Portal<br>III. The Customer may click the hyperlink and view the mitigation in progress | On detection of high severity Misuse Detection Alert |
| **Step 3** Monitoring and diagnostics during a mitigation | NOC & Customer | I. The NOC will continue to monitor the mitigation<br>II. The NOC may need to manually change the template as part of the ongoing mitigation process<br>III. The Customer may call the NOC to review status, discuss progress and request updates<br>**2nd & 3rd Line Involvement**<br>The NOC 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 | NOC | Where mitigation was automated using Sure Attack Mitigation Devices, the mitigation will complete automatically once the high severity Alert has ended. | As advised by the NOC and agreed by all Parties. |
| **Step 5** High severity Misuse Detection Alert condition ended | NOC | I. An automated email will be sent to the Customer Approved Personnel address(es) advising the alert condition has ended, it will contain a hyperlink to the Alert in the Sure Portal allowing the customer to access Alert details as required<br>II. Customers can review reports on all historical Alerts within the Sure Portal | On detection of the end of a high severity misuse alert |

| | | | |
|---|---|---|---|
| **Step 6**<br>Mitigation ended | NOC | I. An automated email is sent to the Customer email address(es) to advise that the automatic or manual mitigation has stopped with a link to the alert in the Sure Portal to allow customer to access alert details if required<br>II. Customers can review reports on all historical mitigations within the Sure Portal | **For Automatic Mitigations** occurs on completion of an automatic mitigation event<br><br>**For Manual Mitigations** will be manually stopped by the NOC |
| **Step 7**<br>Mitigation not successful or cannot be ended | | If an incident cannot be mitigated successfully using the Sure Attack Mitigation Devices then the NOC may request mitigation via the Cloud Partner Facilities. Refer to table **Incident Progression, Resolution and Closure using Cloud Partner Facilities** which replaces Steps 4 to 6 above. | **NOC** |

| Step | Owner | Action | Timeline |
|---|---|---|---|
| **Misuse Detection - Incident Progression, Resolution and Closure - Using Cloud Partner Facilities** | | | |
| **Step 4**<br>Incident Progression using the Cloud Partner Facilities | NOC & Customer & SOC | I. If an incident cannot be mitigated using Sure Attack Mitigation Devices the NOC may request mitigation via Cloud Partner Facilities. Customer's approval or pre-authorisation to use Cloud Partner Facilities is required.<br>II On receipt of valid approval, or confirmation that pre-authorisation is held by Sure, the NOC will liaise with the SOC to invoke Attack Mitigation<br>III. NOC will confirm with the Customer that they are receiving cleaned traffic via the Cloud Partner Facilities. **Note:** Use of Cloud Partner Facilities are generally reserved for volumetric attacks that exceed the capacity of Sure Attack Mitigation Devices. Mitigation using Cloud Partner Facilities is provided in blocks of up to 72 hours | When agreed between Customer & NOC |
| **Step 6**<br>Updates when using Cloud Partner Facilities | Service Manager | Email updates can be provided on a periodic basis as agreed with the customer. | As agreed with the Customer. |
| **Step 5**<br>Incident Resolution & closure | NOC | The NOC and Customer (with support of the SOC) will manage the completion of mitigation and moving traffic off Cloud Partner Facilities, at a time defined by the client, within the 72 hour incident window.<br>**Note:** This may cause a brief period of network interruption due to global BGP routing table convergence. | As advised by the NOC and agreed by all Parties. |

3.3 **The optional Profiled Detection Alert incident response procedure** consists of the following:

A Profiled Detection Alerts is generated following the detection of excessive rates of traffic to an IP address within a Managed Object when compared to the traffic rates that the Sure Attack Mitigation Devices expect. Profiled detection can also detect excessive rates of traffic based on a manually configured Managed Object threshold. When Sure Attack Mitigation Devices detect a profiled anomaly, it gathers details about the anomalous traffic and targeted IP address to include in the Alert.

Profiled Detection can generate false positives (for instance if a large file is transferred across a VPN) and so is provided as an optionally configured service to the Customer on request, from which, the Customer may opt to receive automatic email alerts or to access Alert reports on the Sure Portal. The NOC will not proactively take any action on Profiled Detection Alerts

**3.3.1 Profiled Detection Alert process**

| Step | Owner | Action | Timeline |
|---|---|---|---|
| **Ongoing** | NOC | **NOC monitor service on a 24 x 365 basis** | Ongoing |
| **Step 1** High severity Profiled Detection Alert | NOC | An automated email is sent to the Customer Approved Personnel email address(es) containing a hyperlink to the Alert on the Sure Portal. The customer may access the Sure Portal Alert details as required | On detection of a high severity Profiled Detection Alert |
| **Step 2** Profiled Detection Alert condition investigation | Customer | I. On receipt of the Profiled Detection Alert email the Customer may follow the hyperlink to the Alert on the Sure Portal to identify if this is something that needs further investigation internally.<br>II. The Customer may then call the NOC for assistance and mitigation if the Alert is, or may become, service affecting<br>**Note:** if an attack increases and could flood Customer bandwidth then a Misuse Detection Alert will be raised causing the Misuse Detection Alert Incident Response Process to be initiated | As required during a Profiled Detection Alert by the Customer |
| **Step 3** High severity Profiled Detection Alert condition ended | NOC | I. An automated email is sent to the Customer Approved Personnel email address(es) to advise the Alert condition has ended. The email will contain a hyperlink to the Alert in the Sure Portal to allow customer to access Alert details as required<br>II. Customers can review reports on all historical Alerts within the Sure Portal | On detection of the end of a high severity Profiled Detection alert |

3.4 Sure will use reasonable endeavours to ensure that legitimate traffic is received as normally as possible during any attack, and that the IP Address (es) and DDoS protected Managed Objects 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; off ramp Mitigation using Cloud Partner Facilities may then be used.

3.5 During the mitigation of a confirmed attack, if Sure Attack Mitigation Devices are deemed not to be sufficient;

a. a volumetric attack exceeds the capacity of the Sure Attack Mitigation Devices or
b. a Sure primary IP transit links to the Internet is saturated causing network instability,

then Sure may opt to perform Attack Mitigation using Cloud Partner Facilities to mitigate the attack. Once all parties authorise that Cloud Partner Facilities should be used, traffic will be routed to Cloud Partner Facilities systems, a charge will be made for this service as detailed on the Order Form.

3.6 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

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

3.8 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

3.9 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 On Boarding Document and associated Managed Object configurations
- Non urgent configuration changes requested by the Customer, including changes to monitoring, mitigation template(s) or Managed Objects.
- 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 reports 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**

For issues with the service or performance failures where the Customer believes the Service Levels have not been met the following escalation contacts are available.

| Level | Name | Function | E-mail | Telephone |
|---|---|---|---|---|
| 1 | NOC | Network Operations Centre | noc@sure.com | +44(0)1481 757777 |
| 2 | Confirmed by Assigned Service Manager/Account Director | Service Manager | servicemanagement@sure.com copy datacentresales@sure.com or other such email as provided by your assigned Service Manager | To be confirmed by Assigned Service Manager |
| 3 | Confirmed by the Assigned Service Manager or the NOC | Head of Head of Service Integrity (NOC) and/or Head of Service Assurance (IP Engineering.) | Confirmed by the Assigned Service Manager or the NOC | Confirmed by the Assigned Service Manager or the NOC |
| 4 | Cyrille Joffre | CTIO | cyrille.joffre@sure.com | +44(0)7781 157757 |
| 5 | Eddie Saints | CEO | eddie.saints@sure.com | +44(0)7700 753329 |

**4.5 Engineering configuration changes**

Charges for engineering configuration changes will be made to add new monitored Managed Objects to an existing Sure DDoS Attack Mitigation Service. There will be no Charge for removing redundant Managed Objects. 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 Approved Personnel 24 hours' notice for items listed below:

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

If the Customers Approved Personnel does not respond to Sure's notification to undertake the emergency maintenance, Sure will make the change at a time Sure considers to be most convenient for all Parties.

**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 Approved Personnel to schedule a time to make the necessary changes. The Customers Approved 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 Approved 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. Reporting – The Sure Portal**

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

6.1 The following reporting 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 Managed Object(s), showing current Alerts, Attacks and incoming and outgoing traffic to aid Customer's determine the current status of their Service

6.1.2 Managed Object–level views provide a log of events for the selected Managed Object, including Attack history, durations and types

6.1.3 Historical reports provide a visual record of Attacks and associated Alert responses over the past 3 months for determining Attack patterns and allowing verification of successful protection against Attacks.

The portal will not display reports or mitigation information when Attack Mitigation using Cloud Partner Facilities is invoked. Post DDoS mitigation reports can be provided within 72hrs of the Cloud Partner Facilities Mitigation ending.

**7. Export Control**

7.1 Delivery of the Service to the Customer may be subject to relevant export control law and regulations. Sure do not represent that any necessary approvals and licenses will be granted. The Customer will provide reasonable assistance to Sure to obtain any necessary consent. If, through no fault of Sure, any necessary consent is not granted, then Sure can terminate this Agreement and the provision of the Service under it (as appropriate) without any liability to the Customer.

7.2 The Customer agrees to comply with any applicable export or re-export laws and regulations of any country, including obtaining written authority from the US Government if the Customer intends at any time to re-export any items of US origin to any proscribed destination.

7.3 For US Government personnel using the Service in Guernsey or United Kingdom, US Government restricted rights will apply.

**8. Liability**

8.1 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. Under no circumstances will Sure liability exceed the amount the Customer has paid for the Service in any 12 month rolling period, starting on the Service Delivery Date.

8.2 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 as a whole.

**9. 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 of Managed Objects) | Non Recurring Charge plus Monthly Recurring Charge |
| Attack Mitigation using Cloud Partner Facilities (when agreed by the Parties) | Non-recurring charge at the rate in force (per 72hr mitigation window)<br><br>Indicated on the Order Form |
| Make critical change | Non Recurring Charge |
| Make non-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.

**10. Payment**

10.1 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.

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

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

10.2.2 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.

10.3 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

**11. General Terms and Conditions**

The Customer should refer to the Sure Master Service Agreement or Data Centre General Terms and Conditions and Sure General Terms & Conditions for additional clauses under each of the above headings and in particular for the following:

| | |
|---|---|
| Special Provision of Service | Use of Service |
| Connection of Equipment to the Service | Security |
| Domain Name | Charged Domain name |
| The Network | Common Gateway Interface |
| Intellectual property Rights | Confidentiality |
| Acceptable Use Policy | Export Control |
| Fault Repair | Term of Service |
| Temporary Service | Interconnection |
| Payment | Deposits and Payments in Advance |
| Default | Cancellation |
| Suspension | Termination |
| Call Monitoring and Recording | Accommodation, Power and Lightning Protection |
| Information and Permissions | Access to Premises |
| Complaints and Arbitration | Assignment |
| Copyright | Duration and Entire Agreement |
| Liability | Matters Beyond Reasonable Control |
| Notice | Use of Information |
| Severability | Variation |
| Waiver | Law |

**12. 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 high severity 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 high severity Misuse Detection Alert where automatic mitigation is not configured, or from a Customer requested manual mitigation | 30 minutes from mitigation approval from the Customer |
| Time to mitigation using Cloud Partner Facilities | The time to mitigation with Cloud Partner Facilities following approval provided by Customer | Less than 30 minutes for layer 3 & 4 attacks, plus an additional 10 minutes for layer 7 attacks |
| Fall-Back Procedure (when using the Cloud Partner Facilities) | Should the DDoS Attack Mitigation using Cloud Partner Facilities have an adverse effect on the Customer or Sure services, at the request of Sure, the SOC will return traffic directly to Sure | 30 minutes |

**13. 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. |
| Non-Critical Change | Response: Within 4 working hours<br>Resolution: Within 1 business day (or as agreed with customer) |
| Critical Change | Response: Within 1 hour<br>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 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.

**14. Fault Support for the DDoS Attack Mitigation Service**

| | |
|---|---|
| Fault Support | Is provided via the NOC 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.