HKBN
ENTERPRISE SOLUTIONS

Special Terms and Conditions of AegisConnect – DDoS Protect and Managed Firewall Service ("the Services")

1. Definitions

All capitalised terms used in this document shall have the meaning ascribed in HKBNES's General Terms and Conditions of Service unless the context requires otherwise or defined below:
"**Contract**", in relation to HKBN Enterprise Solutions Limited, means "Agreement" as such term is defined in its General Terms and Conditions.
"DDoS Protect" means AegisConnect DDoS Protect Service and ancillary services as set out in the Application. There are Always-On and On-Demand options.
"**HKBNES**" means either (i) HKBN Enterprise Solutions Limited; or (ii) HKBN Enterprise Solutions HK Limited, as set out in the Contract and includes their successors, transferees, or assignees.
"**HKBNES SOC**" means HKBNES's Security Operations Centre.
"**Managed Firewall Hardware**" means the hardware provided and installed by HKBNES at the premises of a Customer who subscribes for the Managed Firewall Services. This hardware is available for rental from HKBNES by Customer.
"**Managed Firewall Services**" means the optional value-added services offered by HKBNES for subscription by Customer as set out in the Application.
"**Service Term**" means the period during which the Services are provided by HKBNES to Customer.
"**Services**" means either or both of DDoS Protect and Managed Firewall Services as the case may be, unless otherwise stated.
"**SLA**" means any applicable service level agreement in relation to the Services.

2. Provision of Services

2.1 HKBNES will provide the DDoS Protect or/and Managed Firewall Service to Customer subject to the Contract and these special terms and conditions. Customer shall comply with the Contract and these special terms and conditions. For clarity a breach of any provisions in these special conditions will entitle HKBNES to take such action as it sees fit including restricting, suspending, or terminating the DDoS Protect or/and Managed Firewall Service to Customer with or without notice.

2.2 DDoS Protect is an IP-Based DDoS protection service which aims to help Customer to mitigate Layer 3 and Layer 4 DDoS attacks. The maximum amount of clean traffic allowed is limited by the service plan that has been subscribed.

2.3 SLAs do not apply during planned maintenance work. SLAs cannot be guaranteed if Customer does not make the changes required by HKBNES or if Customer otherwise prevents HKBNES from making the changes it notifies Customer are necessary for continued Services.

2.4 Customer who subscribes to DDoS Protect On-Demand is expected to implement HKBNES provided Dedicated Internet Access (DIA) by DDoS Protect as secondary link, for which Customer shall have primary DIA service subscribed. Customer is responsible for any network re-configurations or DNS re-configurations to implement to changeover any incoming traffic from their existing primary link to DDoS Protect secondary link to enjoy DDoS protection, which may include but not limited to route, firewall settings, DNS record etc. HKBNES will not be responsible for any losses incurred during changeover or downtime caused by these Customer-initiated changes.

3. No Guarantee

3.1 Customer acknowledges that deployment of the Services does not achieve the impossible goal of risk elimination, and therefore HKBNES does not guarantee that intrusions, compromises, or other unauthorized activity will not occur on Customer's network.

3.2 Customer may face service degradation or packet loss when under DDoS attack. HKBNES shall not be liable to Customer or any third party for any loss or damage caused by the failure or ineffectiveness of DDoS Protect.

3.3 For DDoS Protect (either Always-On or On-Demand), the platform provides no traffic latency guarantee, as latency performance depends on the network path selection of global or local Internet Service Providers. HKBNES is not responsible for any losses incurred or to troubleshoot with international ISPs in case of high latency issue.

3.4 The maximum amount of traffic that can be protected by the DDoS Protect is limited by the DDoS Protect platform. Only the IP addresses under the DIA Service shall be covered in the DDoS Protect.

4. Changeover (only applicable to Customer who subscribes to DDoS Protect – On-Demand)

4.1 Customer is expected to notify HKBNES whenever there is changeover of the traffic to the link with DDoS Protect which is serving as secondary link. The notification to HKBNES may be given within 24 hours after the changeover. Any changeover without notice may considered as misuse of platform.

4.2 Customer is expected to perform the changeover process. Or if the changeover plan involved in on-boarding service includes process that is/are performed by HKBNES, HKBNES would perform the actions accordingly. As such, one token is consumed. Customer should consider purchasing additional changeover token after consumed.

4.3 Customer is expected to carry out changeover back to primary DIA connection which is non-HKBNES provided DIA service within 24 hours. HKBNES reserves the right to charge on daily basis for extra license incurred at DDoS Protect platform beyond the 24-hour period. If DDoS attack is expected to exceed the 24-hour period, Customer may contact HKBNES to extend for additional 24-hour period and the extension would not introduce extra charge.

5. Managed Firewall Services (only applicable to Customer who subscribes to the Managed Firewall Services)

5.1 Customer agrees to deploy and permit the deployment of the Managed Firewall Hardware solely in connection with the Managed Firewall Services.

5.2 Customer shall comply with the following requirements:

(a) Customer must provide HKBNES access to its premises for HKBNES to install, manage and monitor the Managed Firewall Hardware;

(b) no configuration changes shall be made to the Managed Firewall Hardware except with the prior written approval of HKBNES;

(c) the password on the Managed Firewall Hardware shall be configured only by HKBNES and shall not be changed by Customer;

(d) at all times, the Managed Firewall Hardware shall be and remain stored at the location where it was installed by HKBNES;

(e) Customer shall maintain safeguards against the destruction or damage of or unauthorised use of the Managed Firewall Hardware that are consistent with the normal safeguards maintained in relation to Customer's own property; and

(f) Customer must provide good working connectivity in Customer's designated network for connecting the Managed Firewall Hardware to HKBNES SOC to facilitate provision of the service.

5.3 Any provision of updates and bug fixes for the Managed Firewall Hardware will be at the sole discretion of HKBNES. HKBNES will normally provide software upgrades to the Managed Firewall Hardware by remote administration. Onsite upgrade to the software can be arranged upon request and extra cost may be involved.

5.4 In cases where support for a particular product or product version of the Managed Firewall Hardware is being discontinued by the product vendor or by HKBNES, HKBNES will advise on new platform migration options. In order to ensure uninterrupted service, Customer must complete the migration process within sixty (60) days. Customer bears any costs relating to procuring new hardware or components or re-provisioning of any devices.

6. Connectivity to HKBNES SOC (only applicable to Customer subscribes to the Managed Firewall Services)

6.1 Customer must communicate any network or system changes that may impact service delivery to HKBNES support hotline at least one (1) business day in advance.

6.2 If connectivity failure is Customer related, such as a network change, outage, or customer-managed device, HKBNES will provide Customer with troubleshooting information upon Customer request, but HKBNES is not responsible for trouble shooting issues that are not directly related to the Services.

7. Authorization for Network Access

7.1 Certain laws and regulations prohibit the unauthorized penetration of computer networks and systems. Customer agrees that its subscription for the Managed Firewall Hardware constitutes permitted access by HKBNES to Customer's networks and computer systems.

7.2 Notwithstanding any provision to the contrary, HKBNES shall assume no responsibility for any claims, liability, loss or damages whether directly or indirectly as a result of the Services (including the conduct of penetration tests) under any circumstances, except where due to the wilful default and gross negligence of HKBNES.

8. Change Management (only applicable to Customer who subscribes to the Managed Firewall Services)

8.1 Customer may submit change requests to HKBNES via HKBNES's hotline for the Managed Firewall Services. The change request must be made by an authorised contact of Customer.

8.2 Change request that may be made by Customer is subject to number limits as set out in the particular service package subscribed by Customer.

8.3 HKBNES does not design or validate rule sets or provide troubleshooting related to rule sets as part of the Services.

8.4 HKBNES's responsibilities surrounding application control are limited to enabling or disabling the application control settings.

8.5 HKBNES is not responsible for application debugging in the event of unexpected consequences from application control settings in respect of any software applications used by Customer.

9. Metadata and Logs

(a) During the Service Term, HKBNES will collect metadata and related content generated by incoming traffic towards Customer's network ("metadata") pursuant to the provision of the Services. HKBNES will maintain the metadata for a period of three (3) months from the date the metadata are generated by DDoS Protect. The metadata may include malicious source IP addresses, traffic statistic (BPS, PPS), attack statistic (vector, source, destination, port) and attack type. Customer's data (sensitive/non-sensitive data) or other unrelated traffic content is not being inspected or stored.

(b) For logs generated from Managed Firewall (only applicable to Customer who subscribes the Managed Firewall Services), HKBNES will maintain the copies of the collected logs for a period of three (3) months from the date the logs are generated (or such longer period as expressly agreed by the parties), after which time HKBNES will delete or otherwise render inaccessible the copies of the logs held by HKBNES.

10. Minimum Subscription Period

(a) DDoS Protect shall be subscribed for a minimum period of twelve (12) months.
(b) Managed Firewall Service shall be subscribed for a minimum of period of twenty-four (24) months.
(Respectively, "Minimum Subscription Period")

If Customer terminates the DDoS Protect/ Managed Firewall Service prior to the expiry of the Minimum Subscription Period, Customer shall be liable to pay early termination charges equivalent to the service charges payable for the remainder of the Minimum Subscription Period.

11. Misuse/ Overuse of DDoS Protect

Customer shall review the actual bandwidth consumption and subscribe DDoS Protect with sufficient and suitable bandwidth. The following situations, include but not limited to, are considered as misuse/ overuse:

- Bandwidth consumption usually exceeds the amount of clean bandwidth subscribed.
- DDoS On-Demand Customer usually having significant bandwidth consumption.
- DDoS On-Demand Customer do not changeover back to primary link after an attack mitigation and without any request to extend the 24-hour period.

For any misuse or overuse, HKBNES reserves the right to charge on daily basis for extra license.

12. Consequences of Termination

12.1 On termination of the DDoS Protect, Customer shall:
(a) perform any necessary re-configurations, which may include but not limited to route, firewall settings, DNS records, etc.
(b) HKBNES will delete or otherwise render inaccessible any of the metadata or logs that remain in HKBNES's possession or control;
(c) Upon termination of Services, no additional service to export or extract data for Customer.

12.2 On termination of the Managed Firewall Services:

(a) Customer shall re-configure any necessary configuration change, which may include but not limited to route and firewall settings depends on the setup in Customer's environment.

(b) Upon termination of Managed Firewall Service, Customer shall disconnect the Managed Firewall Hardware from the network and contact HKBNES for on-site collection. within 14 days from the date of termination of Services. The Managed Firewall Hardware should be in good condition (fair wear and tear excepted).

(c) Customer shall return the Managed Firewall Hardware to HKBNES within the specified period after termination of the Services. If Customer fails to return the Managed Firewall Hardware or any part thereof within the specified period or the Managed Firewall Hardware is lost or damaged, Customer shall indemnify HKBNES for all loss or any damages to the Managed Firewall Hardware on a full indemnity basis (including the costs incurred by HKBNES for the recovery of the Managed Firewall Hardware).