HKBN ENTERPRISE SOLUTIONS HK LIMITED ("HKBNES")
Special Terms and Conditions for Asure Security Service

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:

"**Security Gateway Hardware**" means the hardware provided by the Customer which meets the technical specifications and configuration requirements designated by HKBNES for deployment of the Services. This is available for purchase from HKBNES by Customer at Customer's option.

"**Security Gateway Location**" means the location of Customer's designated network at which the Security Gateway Hardware provided by Customer is to be installed and operated.

"**Service Term**" means the period during which the Services are provided by HKBNES to Customer.

"**Services**" means Asure Security Service and ancillary services as set out in the Application.

"**Software**" means any software used to provide the Services which are installed and used by HKBNES on the Security Gateway Hardware.

"**SLA**" means any applicable service level agreement in relation to the Services.

"**HKBNES SOC**" means HKBNES's Security Operations Centre.

2. Provision of Services

2.1 HKBNES will provide the Services 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 clarify 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 Services to Customer with or without notice.

2.2 The provision of the Services by HKBNES is subject to Customer arranging for the following:
(a) Customer must provide the Security Gateway Hardware, for the installation and operation of the Software used to provide the Services;
(b) Customer must provide access to the Security Gateway Location to HKBNES, for HKBNES to install, manage and monitor the Security Gateway Hardware and the Software; and
(c) Customer must subscribe to dedicated link service from HKBNES, for connectivity from the HKBNES SOC to the Security Gateway Location.

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.

3. No Guarantee

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.

4. Security Gateway Hardware

4.1 During the Service Term, Customer agrees to deploy and permit the deployment of the Security Gateway Hardware solely in connection with the Services.

4.2 HKBNES will install the Software on the Security Gateway Hardware for the provision of the Services.

4.3 Customer shall comply with the following requirements:
(a) the Security Gateway Hardware and ancillary facilities will only be configured for TCP/IP Security and will be used solely for HKBNES's related data/log transfers;
(b) no configuration changes shall be made to the Security Gateway Hardware except with the prior written approval of HKBNES;
(c) the password on the Security Gateway Hardware shall be configured only by HKBNES and shall not be changed by Customer;
(d) at all times, the Security Gateway Hardware shall be and remain stored at the location expressly designated by HKBNES as agreed by Customer;
(e) Customer shall maintain safeguards against the destruction or damage of or unauthorised use of the Security Gateway Hardware that are consistent with the normal safeguards maintained in relation to Customer's own property;
(f) Customer shall ensure that there is no sharing of accounts on the web portal for the Services; and
(g) Customer shall promptly (and in any event within three (3) business days of any such change) notify HKBNES of changes in any connection / function requirements of Customer's network (including any changes in hardware or software) by completing and submitting to HKBNES the form as designated by HKBNES from time to time.

5. Software

5.1 HKBNES hereby grants to Customer a licence to use the Software on the Security Gateway Hardware during the Service Term in accordance with the provisions of the Contract.

5.2 Provision of any updates and bug fixes for the Software will be at the sole discretion of HKBNES. HKBNES will normally provide upgrades to the Software by remote administration. Onsite upgrade to the Software can be arranged upon request and extra cost may be involved.

5.3 Customer agrees that the Software may collect and communicate certain software, hardware, and use information to HKBNES or HKBNES's service providers' servers for the purposes of: (i) checking for and performing any updates; (ii) ensuring that Customer has complied and are complying with the terms and conditions in the Contract, including Customer's use of valid software key codes, hardware keys, or both; and/or (iii) tracking and monitoring of security intrusion. The information collected and communicated does not include any proprietary application data. HKBNES will not provide any of the information to any third party except as required by law or legal process or to enforce compliance with the terms and conditions in the Contract.

5.4 In cases where support for a particular product or product version of the Software is being discontinued by the product vendor or by HKBNES, HKBNES will advise on new platform migration options. In order to be assured of 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.

5.5 Customer agrees that HKBNES and/or its suppliers have and will retain all rights, title and interest in and to the Software, including any intellectual property rights therein. Customer agrees it will not: (i) make any copies of the Software; (ii) reverse engineer, decompile, or disassemble the Software; (iii) sell, resell, transfer, license, sublicense, or distribute the Software; or (iv) create, write, or develop any derivative software or other software program that is based on the Software.

6. Connectivity to HKBNES SOC

6.1 Customer must provide good working connectivity in Customer's designated network for connecting the Security Gateway Hardware to the dedicated link service subscribed by Customer from HKBNES for connection to HKBNES SOC to facilitate provision of the Services.

6.2 Customer must communicate any network or system changes that may impact service delivery to HKBNES SOC via a ticket in HKBNES's customer portal at least one (1) business day in advance.

6.3 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 Security Gateway Hardware under HKBNES's operation.

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 Services constitutes permitted access by HKBNES to Customer's networks and computer systems.

7.2 If one or more of the IP addresses identified by Customer is or are associated with computer systems that are owned, managed, and/or hosted by a third party provider ("Host") or if any third party consents are so required for any other reason, Customer shall procure and warrants that it has the consent and authorization from such Host(s) or third parties necessary for HKBNES to provision the Services.

7.3 Customer shall facilitate any necessary communications and exchanges of information between HKBNES and such Host(s) or third parties.

7.4 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

8.1 Customer may submit change requests to HKBNES via HKBNES's customer portal for the 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. Logs

During the Service Term, HKBNES will collect copies of logs, data and other related content generated by Customer's network equipment ("Logs") pursuant to the provision of the 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. Customer shall make its own arrangement for collecting and retaining copy of any Logs for its own reference purpose.

10. Minimum Subscription Period

Customer shall subscribe the Services for a minimum subscription period of twenty-four (24) months ("Minimum Subscription Period"). If Customer terminates the Services 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. Consequences of Termination

On termination of the Services, Customer shall:
(a) no longer have rights to access the Software or use the Services or associated instructional manuals or materials. At Customer's request and for a period of up to 14 days from the date of termination of Services, HKBNES will make available to Customer the Logs as existing in respect of the Services on the date of termination. At the end of such 14 days period, and except as may be required by law, HKBNES will delete or otherwise render inaccessible any of the Logs that remain in HKBNES's possession or control;
(b) de-install, or permit HKBNES to de-install, the Software from the Security Gateway Hardware; and
(c) return or destroy the media and all documentation associated with the Software promptly upon the written request of HKBNES and certify in writing to HKBNES (or its Software licensors if HKBNES so directs) that the Software have been de-installed and the media and all documentation have been returned or destroyed, if so requested by HKBNES.

END