

Special Terms and Conditions of Aegis DNS Security Easy Protect Service (“the Services”)

1. Aegis DNS Security Easy Protect Service (“Service”) is a cloud-delivered service that designed to provide DNS-layer security solution for Customer with 25 users or below and their devices connected to the Internet and proactively identify and block malware and phishing sites. HKBNES will engage a designated vendor (“Vendor”) as a sub-contractor to support the Service. Customer agrees and acknowledge that its IP addresses will be registered in Vendor’s platform to protect the Customer’s outgoing internet traffic against attacks. Customer shall understand the terms and conditions implemented by the Vendor (Cisco) (please refer to https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco-Umbrella-Enterprise-Terms-of-Service.pdf).
2. HKBNES has the right to change the Vendor.
3. HKBNES will use reasonable endeavors in providing the Service to detect all known malwares and phishing sites accessed on the Internet by the Customer but does not guarantee that it will be continuous and completely fault-free or all malwares and phishing sites will be promptly detected and restricted at all.
4. Customer shall change the DNS (domain name system) setting in either router / gateway or firewall (if any) or configure it in the device setting and forward the DNS queries to the Vendor. For bundled router, HKBNES will assist the Customer in configuring the DNS set up during broadband installation. For non-bundled router, HKBNES will use its reasonable endeavours to assist in the setting up during broadband installation and will only handle the set-up when the Customer allows HKBNES employees, contractors, or agents of HKBNES to access the equipment and/or router with administration login (if necessary). HKBNES shall not be responsible for any loss or damages suffered by the Customer during the set-up.
5. If Customer alters the DNS setup, bypasses the Umbrella DNS in any way, or uses its own DNS setting to access the website, Umbrella security protection will not be available. If the end-device or any of the LAN network routing devices has been installed or configured for any other URL filtering software/ service, it may interfere with Umbrella security protection. If Customer terminates the Service, Customer shall change the DNS setting and DNS queries from the Vendor.