For Immediate Release

HKBN Introduces Decisive Measures to Delete Sensitive Data from over 3 Million Customer Records in 3 Months

(Hong Kong – 23 April 2018) Hong Kong Broadband Network Limited ("HKBN" or the "Company") announced last week that it had suffered a targeted hacking attack, resulting in unauthorized access to an inactive customer database, and it had reported the case to the Police and Office of the Privacy Commissioner for Personal Data ("PCPD"). Today the Company announced decisive measures to make its retained database far less attractive to hacking in the future, as well as a series of network security enhancement initiatives.

HKBN will collect and retain far less customer data for all its new customers, and will also remove partial data retrospectively for all its customer records. To implement within the coming 3 months, HKBN will delete from its database all personal data of customers whose accounts have been closed and cleared for 6 months. The Company will only retain partial but not the full numbers of HKID card and credit card for all its existing customers. In light of the ongoing processes in relation to the unauthorized access, and to ensure compliance with its operating licenses, HKBN will seek the views of the relevant authorities on these initiatives before it proceeds.

For all new customers, their full identity card number and credit card number will be collected only to support service activation, number porting and bank payment application. Once these procedures are complete, part of the said two numbers will be deleted from the HKBN system.

William Yeung, Co-Owner and CEO of HKBN said, "To regain Hongkongers' trust, we must take immediate and decisive actions beyond industry's common practice to protect our customer data from future attacks. To address the root cause, we will not ask for or retain personal data beyond what is absolutely required by law and business operation. Keeping only partial but not all of the most sensitive data like credit card number and HKID card number gives peace of mind to our customers and also makes HKBN a far less attractive target for hackers."

While the investigation/enquiry by the authorities and HKBN's network security consultant PwC is on-going, William Yeung said, "No conclusion of the incident investigation is available yet, but we've already identified the areas that we will definitely address on to enhance data security protection, such as introducing multiple-factor authentication, stepping up encryption, putting up additional layers of cyber defences on top of our existing protections, and burgeoning resources to expand the

Information Security Team."

HKBN customer data retention policy

Customer personal data	**New policy**	**Implementation timeline**
All personal data of customers whose account is closed and cleared	• Kept for **6 months**, and **delete** afterwards	**Completes in 3 months** (subject to feedback from the relevant authorities)
HKID number of existing customers	• Instead of keeping the full HKID number, **randomly remove 2 out of 6 digits and the bracketed digit** e.g. A12xx56(x)	
Credit card number of existing customers	• Instead of keeping the full 16-digit credit card number, **remove 6 digits** e.g. 1234 56xx xxxx 5678 • Use of "**token**" instead of card number to support payment transactions with banks	

- End -