Guidance for Security against Fraudulent Use of PCCW Conferencing Service

The following notes are provided as the guidance for the best practice in managing your PCCW Conferencing Account(s) to reduce its exposure to possible fraudulent use.

1. Conference code and Leader PIN should be changed every three months.
2. Telephone extension numbers and staff or ID numbers should not be used as Conference code or Leader PIN.
3. Discourage staff from writing down their Conference code and Leader PIN.
4. The Private Plus Dial-Out service should only be allocated to authorized members of staff on a ¡genuine need¡ basis.
5. Access to the Private Plus Dial-Out service should be restricted by a Leader PIN.
6. Leader PIN for Private Plus Dial-Out service access should be allocated to each authorized member.
7. Ensure that staffs sign non-disclosure agreements regarding their Leader PINs.
8. Monitor the usage on charged telephone calls, such as IDD calls.
9. Immediately cancel or change the Conference code and Leader PIN of any staff who leaves the company.

The above advice and guidance are given in good faith for your general information only. You are advised to develop your own safety measures to prevent any possible fraudulent use of PCCW Conferencing Service.