Sun*	**CONFIDENTIAL INFORMATION COMMITMENT IN USING CORPORATE DEVICES OUTSIDE THE COMPANY'S AREA**	No: BM-2-011-09
		Version: 01
		Date issued: 30/07/2019
SUN ASTERISK VIETNAM CO., LTD		**ISO/IEC 27001:2013 & ISO 9001:2015**

Full name: ..... Unit/Department: .....

Devices for request	MAC address
.....	.....
.....	.....
.....	.....

Reason:	

Employees are allowed with the right of using the corporate devices outside the company's area only when employees understand the content and complete signing this confidentiality commitments.

In addition to ensuring full responsibility & commitment to the contents of the Labor Contract signed on the first working day, employees commit to correctly implement the following contents:

DURING USING CORPORATE DEVICES OUTSIDE THE COMPANY'S AREA:

- Employees commit to ensuring the safety of devices which are allowed to bring outside the company and returning them when the deadline comes.
  In case borrowing the devices for the remote working, employee has to return to the General Affairs Line at the end of the process.
  In case the devices are lost, broken ... employee is under full responsibility according to Company's assets management Procedure.
- Employees commit to ensuring the safety of the confidential information which is in the requested devices.
- Employees limit remote access in the public place or not being secure in terms of network security: cafe shop, internet shop...
- Employees commit to obeying the Company's Information Security Regulation
  Reference as following:
  - Install Anti Virus and enable Firewall for all operating systems *(Windows, MAC, Ubuntu);*
  - Prohibit installing and using software in the high-risk software category, including but not limited to the following groups of software:
    + *Software for remote machine control;*
    + *Screen recording / capture software, reading service, file sharing, source code that has features stored on the Internet: Pastebin, Json Viewer, Gyazo,...;*
    + *Proxy software, OpenVPN software, HotspotShield software,... to bypass the Company's security system;*
    + *Software for tracking and collecting unauthorized data: Keylogger,...;*
    + *Virtual machine settings: Kali Linux, Backtrack,...;*
  - Prohibit attacking the system of the Company and users;
- Employees pay attention to clicking on links that are no assurance.
  In case you have report that the device shows signs of instability (virus infection....), disconnect from the network and notify IFU staff immediately.
- In case that this personal device is stolen or lost, employees are responsible for informming to the responsible PSM/LM, IFU department and ISO secretariat.
- In case of breaking any commitment in this document, I will be fully responsible for resolving the consequence and accept any treatment in accordance with the curent law.
- **This commitment is signed once time and valid during the period when employees are working and using personnal devices to access to local network in the Company.**

Ha Noi / Da Nang/ Ho Chi Minh, day ..... month ..... year .....

Employee

(Signature and full name)