	COMMITMENT TO CONFIDENTIALITY IN THE PROCESS OF USING PERSONAL DEVICES FOR WORK	No: BM-2-800-07
		Version: 06
		Date issued: 02/08/2021
SUN ASTERISK VIETNAM CO., LTD		ISO/IEC 27001:2013 & ISO 9001:2015

Full name: Unit/Department:
Registration term: From.....to.....

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

Reason:	
---------	--

Employees are allowed to bring personal devices, access the company's internal network or use them for work purposes (for testing process) only when employee understand the content and complete signing this confidentiality.

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 AND ACCESSING PERSONAL DEVICES AND ACCESSING THE COMPANY'S INTERNAL NETWORK:


- Employees commit to providing accurate information for the process of using personal devices and the process of connecting to the company's internal network.
- Employees commit to ensuring the personal device is formatted before to connect to the company's internal network in accordance with the company's issued Information Security regulations.

Refer to some of the 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 attack that affects the Company's bandwidth (*such as installing download accelerators software, shareware P2P,...*);
- Prohibit attack the system of the Company and users;
- Don't use company's networks to self-broadcast wifi.

DURING USING PERSONAL DEVICES FOR THE PROJECT TESTING PROCESS:

- Employees must strictly comply with the followings on working:
 - *To attend to the login accounts on the personal device used. To ensure that all product data is not shared publicly to the outside unintentionally;*
 - *Prohibit using personal accounts during testing. All accounts used on the test app or for testing purposes must be mail accounts with the Company domain @sun-asterisk.com or @sun-asterisk.vn provided by the company;*
 - *Check and log out of all accounts when the test time expires. To avoid the mistake between personal email account with Company domain & testing account;*
 - *To attend to turn off the synchronization of images and data related to the product with your personal account during testing. Delete all image/video data after the test is complete and before re-enabling the sync function;*
 - *Comply with regulations on software installation in the Company;*
 - *Note:*
 - Don't install malicious applications by mistake, or install external applications App Store, Google Play...;*

	COMMITMENT TO CONFIDENTIALITY IN THE PROCESS OF USING PERSONAL DEVICES FOR WORK	No: BM-2-800-07
		Version: 06
		Date issued: 02/08/2021
SUN ASTERISK VIETNAM CO., LTD		ISO/IEC 27001:2013 & ISO 9001:2015

- *Limit personal device connections to public or vulnerable Internet sources, not private (at the cafe, free wifi ...) during testing;*
- *Prohibit using product data, data related to actual user information in the production environment to perform tests without the Customer's permission.*

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 the personal devices are stolen or lost, employees are responsible for reporting 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 current law.
- **This commitment is signed once time and valid during the period when employees are working and using personal devices to access to the local network in the Company.**

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

Employee

(Signature and full name)