Republic of the Philippines
Department of Health
Center for Health Development of Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER

22 March 2024

HOSPITAL MEMORANDUM

NO. 116 s. 2024

TO : ALL HOSPITAL PERSONNEL

SUBJECT : PORTABLE DEVICES AND BRING YOUR OWN DEVICE (BYOD) POLICY

An organization's decision to allow employees to use their personally owned devices for work-related activities is known as a ***bring your own device (BYOD)***. BYOD increases internal efficiency, fosters a culture of excellence, and enhances employee satisfaction while ensuring the sustainability of our operations. The use and advantages of devices in an organization are endless, but SPMC must also carefully manage possible threats and security risks that BYOD presents as hackers target remote workers more and more. By taking smart steps, IHOMS Guidelines and Policies s.2023, reaffirmed these further as follows:

1. All personal laptops, mobile phones, tablets, and any other personal portable devices must be secured (protected) while connected to SPMC network. Proper security is dependent on risk factors and available resources at specific locations throughout SPMC. Security may be provided by applying software security check and authentication on all personal devices that will connect to SPMC network.
2. Keeping information stored on a Portable Computing Device secure and current is the responsibility of the person who has the device in his or her possession and control. Those in possession are responsible for breaches of security related to devices in their possession.
3. All portable devices owned by SPMC, and other personal devices allowed on the SPMC network must be registered to SPMC wireless controller for profiling and security measures.
4. All personal devices that would like to connect to SPMC network must undergo software security audit before registration to avoid possible threats to the network. (Software checklist provided)
5. Access rights to the SPMC network cannot be transferred to another person even if that person is using an allowed computing device.
6. All systems containing sensitive information should enable auto log-off capabilities if available. The delay should be determined based upon the risk criteria.
7. Employees, non-employees, and outside vendors/suppliers are required to have appropriate clearance prior to access to computer workstations.
8. Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs, by employees is prohibited when connected to SPMC network. Software required for end user purposes must be approved and installed by IHOMS. The end user must document and maintain proof of license to have such applications.
9. All portable workstations must be equipped with security hardware and/or software. Where appropriate, all workstations and portable devices must be equipped with updated software for detecting the presence of malicious software (e.g. computer viruses).
10. All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

11. The installation of anti-virus software and perform patch updates in personal device is the responsibility of the owner, except if the device is provided by SPMC where IHOMS is the one in-charge in the installation and update.
12. Access to the hospital systems and network from outside of SPMC premise must be controlled by privileged access controls that may only be established by IHOMS through its own firewall and VPN.
13. It is the responsibility of the users with remote access privileges to ensure that remote connection to SPMC is not used by non-authorized individuals to gain access to company information or to internal networks. System provider engineers with remote server access privilege have responsibility to employ security protections that can prevent their computing device from passing along viruses or similar internet threats to the SPMC network and data.

To ensure adherence to these standards, IHOMS shall implement current procedures to monitor personnel's device and its activity. Sanctions are applied when any of these policies are not followed: **Disabling of Access to SPMC Network Connections.**

This Order shall take effect immediately.

RICARDO. B. AUDAN, MD, FPAFP
Medical Center Chief II