Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029

30 May 2014

HOSPITAL ADMINISTRATIVE ORDER
No. 14 s. 2014

TO : ALL CONCERNED

SUBJECT : GENERAL GUIDELINES & COMPUTING POLICIES

1. INFORMATION SECURITY

The Information Security Policy recognizes that not all offices within the Southern Philippines Medical Center are the same and that data are used differently by various concerned office within the SPMC. The principles of intellectual freedom and free exchange of ideas apply to this policy, and this policy is not intended to limit or restrict those principles. Each office within the SPMC should apply this policy to meet their information security needs. The Policy is written to incorporate current technological advances. The technology installed at some office may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the chief information officer or the equivalent officer(s).

A. DATA CLASSIFICATION

It is essential that all SPMC data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. We have specified three classes below:

- High Risk:

Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Payroll, personnel, financial, drug testing and hospital (HIS) information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to SPMC if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

- Confidential:

Data that would not expose the SPMC to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

- Public:

Information that may be freely disseminated All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the Department. · Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

· No SPMC owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

· Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.

· High risk data must be encrypted during transmission over insecure channels.

· Confidential data should be encrypted during transmission over insecure channels.

· All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

· Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

B. ACCESS CONTROL

· Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
· Where possible and financially feasible, more than one person must have full rights to any SPMC owned server storing or transmitting high risk data. The offices and SPMC Administration must have a standard policy that applies to user access rights. This will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data.
· Access to the network and servers and systems should be achieved by individual and unique logins, and should require authentication. Authentication includes the use of passwords, biometrics, or other recognized forms of authentication.
· users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to SPMC-related documents or files is required specifically and solely for the proper operation of end-user's computer units and where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit or section chief and submitted to IHOMP for approval. All users must secure their username or account, password, and system access from unauthorized use.
· All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by IHOMP after consultation with the end-users. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by IHOMP.
· Passwords must not be placed in emails unless they have been encrypted.
· Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
· Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
· Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the project system administrator.
· Transferred employee access must be reviewed and adjusted as found necessary.
· Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
· Activities performed as administrator or super user must be logged where it is feasible to do so.
· Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

C. ACCEPTABLE USE

Each Office or unit must have a policy on appropriate and acceptable use that includes these requirements:

· SPMC computer resources must be used in a manner that complies with SPMC policies and regulations. It is against SPMC policy to install or run software requiring a license on any SPMC computer without a valid license.

· Use of the SPMC's computing and networking infrastructure by SPMC employees unrelated to their SPMC positions must be limited in both time and resources and must not interfere in any way with SPMC functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.

· Uses that interfere with the proper functioning or the ability of others to make use of the SPMC networks, computer systems, applications and data resources are not permitted.

· Use of SPMC computer resources for personal profit is not permitted except as addressed under other SPMC policies.

· Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Security system administrators in the performance of their duties may also use them. They must not be used to monitor or track any individual's network activity except under special authorization as defined by SPMC policy that protects the privacy of information in electronic form.

D. DATA CENTER ACCESS

· IHOMP shall validate the employee requiring access has been made aware of all policies and guidelines that pertain to IHOMP Data Center. Requesting employee\guest may also be held liable for any action or damages against IHOMP Data Center. IHOMP management staff reserves the right to revoke access to the area(s) at any time, for any reason,

· Access to secure areas such as the data center and UPS room must be adequately controlled and physical access to buildings should be restricted to authorized persons. Staff working in secure areas should challenge anyone not wearing an SPMC I.D. (or equivalent identification tag). Each department must ensure that doors and windows are properly secured.

· Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted.

· Data Centre and UPS Room area keys and lockable IT cabinets are held centrally by IHOMP section, as appropriate.

· Use log book provided for the Data Centre and UPS room. All access should be logged, even when a group of persons enters the area.

· Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. IHOMP employee must monitor all visitors accessing secure data centre areas at all times.

· Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorized to access those areas and should not be loaned/provided to anyone else.

· Alarms fitted and activated outside working hours.

· Security camera must be working with recording 24/7

· Ensure only authorized technicians complete any work on the equipment.

- Record details of all remedial work carried out.
- Identify any insurance requirements.
- Record details of faults incurred and actions required.

· The secured area should only be accessed to meet a business requirement. When such a requirement is complete, leave the area. Do not loiter.

· A resource in use (computer, monitor, keyboard, network cable, power cable, cabinet, floorboard, etc.) should be moved only by the person directly responsible for that resource.

· The secured area should only be accessed to meet a business requirement. When such a requirement is complete, leave the area. Do not loiter.
· A resource in use (computer, monitor, keyboard, network cable, power cable, cabinet, floorboard, etc.) should be moved only by the person directly responsible for that resource.
· A resource in use must be properly placed / installed inside the Data Center. Any violation from any IHOMP administrators will be reprimanded and/or revoke access to the data centre.
· Temporary use of cables and the likes are strictly not allowed inside the Data Center for more than five (5) days. Any violation from any IHOMP administrators will be reprimanded and/or revoke access to the data centre

· Food, drink or other fluids must not be introduced to the secured areas.
· Access control mechanisms fitted to all accessible doors (where codes are utilized they should be regularly changed and known only to those people authorized to access the area).

E. SERVER SECURITY

All equipment must comply with the following configuration policy:
Configuration Guidelines
· Server Operating System (OS) configuration must be in accordance with the standard set by the IHOMP, SPMC Senior Administrators.

Standard Operating Procedures
1. OS must be licensed to SPMC
2. OS must be registered to avoid inconveniences during operation
3. OS installation software must be backup and paper license photocopied
· Any servers must not be connected to SPMC network during installation and configuration of hardware, OS and patch updates.
· The most recent security patches must be downloaded and installed on the system right after the installation of SPMC Enterprise licensed Anti-Virus software.
· Services and applications that will not be used must be disabled where practical.
· Do not use administrator/root/super user account when a non-privileged account will do.
· Always create and use your personal Administrator account or based on the account registered in SPMC System.
· Production servers must be properly secured and properly installed physically inside the SPMC data center server rack cabinets. It must be physically located in an access-controlled environment.
· Configuration testing is strictly prohibited on Production Servers such as Database, DNS, Web, etc.
· If a methodology for secure channel connection is available, privileged access must be performed over secure channels, using encrypted network connections such as SSH or IPSec or IHOMP console access independent from the DMZ networks.
· Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
· Production Servers are specifically prohibited from operating from uncontrolled cubicle areas.
· Server rack cabinets should be lock when it is not being access
physically.
· Vendors/suppliers or non-employee of IHOMP-SPMC are not allowed to access any server inside the console area and main data center without proper request and approval.
· Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.
· All applicable security patches/hot-fixes recommended by the vendor/supplier must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.

· Server Operating systems of all hosts internal to the DMZ running Internet Services must be configured to the secure host installation and configuration standards.
· Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.
· Use the log book provided for the Servers and Data Center operation.

Monitoring

· All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
1. All security related logs will be kept online for a minimum of 1 week.
2. Daily full backups will be retained for at least 2 weeks to 1 month.
· Security-related events will be reported to Senior Administrators, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
1. Port-scan attacks
2. Evidence of unauthorized access to unauthorize application and website.
3. Anomalous occurrences that are not related to specific applications on the host.

F. WORKSTATION SECURITY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including protected health information and that access to sensitivity information is restricted to authorized users.
· Employees or end-users using workstations shall consider the sensitivity of the information, including protected SPMC information that may be accessed and minimize the possibility of unauthorized access.
· SPMC will implement physical and technical safeguards for all workstations that access electronic protected SPMC information to restrict access to authorized users. Appropriate measures include:
· Restricting physical access to workstations to only authorized personnel.
· Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
· Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
· Complying with all applicable password policies and procedures.
· Ensuring workstations are used for authorized business purposes only.
· Never installing unauthorized software on workstations.
· Storing all sensitivity information, including protected SPMC information on network servers
· Keeping food and drink away from workstations in order to avoid accidental spills.
· Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
· Complying with the Portable Workstation and BYOD policy
· Complying with the Virus Prevention Policy
· Complying with the Anti-Virus policy
· Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
· Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents
· Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
· If wireless network access is used, ensure access is secure by following the Wireless Access policy

Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029

G. PORTABLE WORKSTATION and BYOD Policy

This includes but is not limited to desktop computers, laptops, iPad, Smartphones and tablets.

· All laptops and any other portable computer equipment must be secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations throughout SPMC. Security may be provided by locking the equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight in a desk or brief case may be appropriate.

· 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

· All portable devices owned by SPMC or allowed on the SPMC network must be identified by their MAC address to the IHOMP before being connected

· The device operator must be identified by name and contact information to the IT department.

· The computer device operator must be familiar with SPMC acceptable use policy.

· BYOD devices are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time. Only SPMC intranet systems (HIS, PACS, Inventory) are allowed to be accessed for authorize BYOD devices.

· Access rights to SPMC network cannot be transferred to another person even if that person is using an allowed computing device.

· All systems containing sensitive information should enable auto log-off capabilities if available. The delay should be determined based upon the risk criteria.

· Employees, non-employees and outside vendors/suppliers are required to have appropriate clearance prior to access to computer workstations.

· Password Protection:

· 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.

· Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs, by employee is prohibited. Software required for end user purposes must be approved and installed by IHOMP. The end user must document and maintain proof of license to have such applications. Software installations will be coordinated through Information Services by calling IHOMP.

· 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). All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

· The installation of virus protection programs and patch updates is the responsibility of the user, except where a user device is connected to the SPMC network, which will install and run appropriate antivirus protection.

· Vendors/suppliers, consultants, and all others wishing to connect portable computing devices to the SPMC network must first submit the equipment to IHOMP for inspection of the adequacy of anti-virus software and installation of critical operation system updates. Contact the IHOMP to initiate this process.

· Users should contact the IHOMP for more information or assistance if they feel that their portable computing device contains particularly sensitive information requiring higher levels of protection.

· Access to any SPMC computer systems from remote locations must be approved by the administrative officer of the concerned office, and the IHOMP. If a remote access system utilizes a dial-up modem, broadband, etc. It must be expressly configured to provide secure network access.
· Access to SPMC internal network from outside of its defined network perimeter must be controlled by privileged access controls that may only be established by the IHOMP. Users are not authorized to install connections such as modems, PC Anywhere, VNC, Team Viewer, etc. Dial-in access and Virtual Private Network (VPN) for 3rd party systems provider connections should be strictly controlled using IHOMP firewall.
· It is the responsibility of users with dial-in access and VPN privileges to ensure that a dial-in 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.

H. VIRUS PREVENTION

· The willful introduction of computer viruses or disruptive/destructive programs into the LAN, WLAN, WAN and VPN environment is prohibited, and violators may be subject to disciplinary action and termination.
· All desktop systems that connect to the SPMC network must be protected with approved, licensed anti-virus software that it is kept updated by the end-user and/or network group administrators.
· All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with approved, licensed anti-virus software that it is kept updated by the end-user and/or network group administrators.
· All incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
· Where feasible, system or network administrators should inform users when a virus has been detected.
· NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
· Delete spam, chain, and other junk email without forwarding to other employee's emails.
· Never download files from unknown or suspicious sources.
· Avoid direct disk sharing with read/write access unless there is absolutely an official requirement to do so.
· Always scan a USB drive from an unknown source for viruses before using it.
· Back-up critical data and system configurations on a regular basis and store the data in a safe place.

I. ANTI-VIRUS

A virus is a piece of self-replicating code, most often a malicious software program designed to destroy or corrupt information or adversely impact the usage of IT systems. Some viruses cause no damage apart from reproducing, but a significant number are specifically designed to cause data loss, compromise the confidentiality of files or disrupt network functioning. Potential sources of viruses include shared media such as CD\DVD-ROMs or USB drive/memory sticks, electronic mail (including, but not limited to, files attached to messages), malicious code embedded in web sites and software or documents copied over networks such as the internal network or the Internet. A virus infection is almost always costly to SPMC whether through the loss of data (possibly permanent); staff times to recover a system, or the delay of important work. Also, viruses spread from SPMC could potentially lead to serious issues. IHOMP will provide the anti-virus software for PC's and will assist individuals in installing the software so that it operates according to the standard. IHOMP will install anti-virus software on all

SPMC owned and installed PC's. IHOMP will take appropriate action to contain virus infections and assist in their removal. In order to prevent the spread of a virus, or to contain damage being caused by a virus, IHOMP may remove a suspect computer from the network or disconnect a segment of the network. Infected machines will be cleaned or reimaged before reconnection to the network.

· All SPMC systems, vulnerable to attack by malware must be protected by antivirus software wherever possible unless a specific exclusion has been granted and alternative measures have been taken to provide the same degree of protection.

· All computers that are connected to SPMC network must have the standard supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus definition files must be kept up-to-date regularly via SPMC Internet or antivirus server.

· All PC's are to be configured such that they schedule regular updates from the Network Services centralized anti-virus servers.

· Any activities with the intention to create and/or distribute malicious programs into SPMC's network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

· Virus-infected computers are removed from the network until they are verified as virus-free.

· Noted exceptions: Unix or Linux operating systems do not have supported anti-virus software supplied by the SPMC, it is the responsibility of the owner/operator of the Unix/Linux system to protect their system from viruses.

· Users using SPMC computers should adopt the following 'best practice' at all times.

1. Exercise extreme caution when opening attachments and check for viruses before opening.
2. Exercise caution when copying files. Only download from reputable sites, and carry out a virus check on the file.
3. Exercise caution when opening files from removable media such as USB drive\memory sticks or CD -ROMs.
4. Scan all external media for viruses before using.
5. Report any virus found to IHOMP Office. Provide the following information if known: virus name, extent of infection, source of virus, and potential recipients of infected material.
6. If possible, warn people to whom the virus may have been sent. Include the name of the virus in the warning if at all possible.

· Users who are authorized to attach their own computer to SPMC network must ensure that their computer has virus protection, which complies with the standards, set out in this policy.

J. WIRELESS (WiFi) ACCESS

· All wireless access points and wireless devices connected to SPMC network must be registered and approved by IHOMP designated representative. All wireless devices are subject to IHOMP audits.

· Only wireless devices approved by make and model shall be used.

· All wireless devices must be checked for proper configuration by the IHOMP prior to being placed into service.

· All wireless devices in use must be checked monthly for configuration or setup problems.

· When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point

· Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

· Laboratory device Service Set Identifier (SSID) must be different from SPMC production device SSID.

· Broadcast of lab device SSID must be disabled.

· Change the default SSID name

· Change the default login and password

· Be installed, supported, and maintained by an approved IHOMP support team.

· Use SPMC approved authentication protocols and infrastructure

· Use SPMC approved encryption protocol

· Maintain a hardware address (MAC address) that can be registered and tracked.

· Not interfere with wireless access deployments maintained by other support organizations.

K. INTRUSION DETECTION

Covers every host on SPMC network and the entire data network including every path that SPMC data may travel that is not on the internet. Paths covered by this policy even include SPMC wireless networks. Other policies cover additional security needs of SPMC network and systems.

· Intruder detection must be implemented on all servers and workstations containing data classified as high risk.

· Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

· Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

· Intrusion tools should be installed where appropriate and checked on a regular basis.

L. INTERNET SECURITY

· All physical Internet connections or connections to other private networks shall be authorized and approved by IHOMP. Most users will access the Internet through the connection provided for their office by IHOMP. Any additional request connections must be approved by IHOMP.
These additional connections include but are not limited to modem, Fax machine, Multipurpose printing machine, wireless access point or devices with wireless capability.

· Any additional Internet connections not provided by IHOMP must be reviewed and approved by IHOMP. Typically any additional connections from SPMC network to the Internet or other private network will require encryption and approved firewall operating at all times and properly configured.

· All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.

· SPMC users are strictly not allowed to use anonymizer applications and download software such as TOR, Ultrasurf, Torrents, Psiphon, Internet download manager etc.

· SPMC users are not allowed to use any network software tools without proper approval of IHOMP.

· Users are not allowed to install and configure any network hardware and software, either knowingly or unknowingly without proper coordination with IHOMP to avoid disruption of SPMC Internet.

· All employee use of the internet shall be for official purposes only.

· Employee use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.

· Employees are urged to use caution when visiting unknown Internet sites and through user training set and keep their browser configured to IHOMP approved standards in order to protect against infections of malware.

· Employees are strictly not allowed to visit inappropriate, pornographic, or dangerous web sites. The IHOMP system shall be able to log the time of Internet activity, duration of the activity, the web site visited, any data downloaded and the type of data downloaded. The activity reports shall compile by IHOMP to support a warning letter issued and for litigation purposes.

M. SYSTEM SECURITY

· All systems connected to the Internet should have a vendor-supported version of the operating system installed.

· All systems connected to the Internet must be current with security patches.

· System integrity checks of host and server systems housing high-risk SPMC data should be performed.

Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029

VII. SUPPORTING POLICIES FOR SPMC LDAP

These policies are not to impose restrictions that are contrary to SPMC's established culture of openness, trust and integrity. SPMC is committed to protecting all end-users, partners and the department from illegal or damaging actions by individuals, either knowingly or unknowingly. These rules are in place to protect the employee and SPMC. Inappropriate use exposes SPMC network to risks including virus attacks, compromise of network systems and services, and legal issues.

EMAIL Policy

· Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
· Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
· Unauthorized use, or forging, of email header information.
· Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
· Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
· Use of unsolicited email originating from within SPMC networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by SPMC or connected via SPMC's network.
· Postings by employees from an SPMC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SPMC, unless posting is in the course of employee duties.
· Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

VIII. TECHNICAL SUPPORT

IHOMP is responsible for maintaining the SPMC network domain.
1. Contact Information
· For SPMC ICT Information Policies; Database; Network, Internet, Wireless LAN Repair & Troubleshooting call Trunk Line No.: 2272731 local 4613
2. IHOMP Group eMail (spmcihomp@gmail.com)
All employees of the IHOMP office are members
of this group and available for technical support.
3. IHOMP Forms
In case, any SPMC users \ clients experience any computer problem regarding
network and Internet connectivity. Please fill up and submit the approved IHOMP
Form 1 "ICT Technical Assistance Request Form" or IHOMP Form No.2 "Service Request Form" to any IHOMP staff. The IHOMP forms are available at
the IHOMP office, JICA OPD bldg. local 4613

Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029

The ICT Technical Assistance Request Form coverage:

· Network Configuration (Router, switches, server, workstation)
· Database
· Firewall Policy
· Backup (Database or Server Services, Etc.)
· Inspection of ICT Equipment
· Network Support
· LAN Cabling (Transfer or Additional)
· Inspection of Equipment for Condemn
· Installation of Anti-virus
· WiFi Setup and Configuration
· SPMC Data Center Site Visit (School\University\Company)
· All major parts of the computer and accessories, printers, scanners, etc.
· Technical actions such as diagnose, repair, scan, installation, configuration/reconfiguration, network connection and troubleshooting
· Technical requirements needed from the clients\users such as buying spare parts, for outside repair, upgrade of computer parts, etc.

The Service Request Form Coverage

- HIS
- LIS
- PACS
- All DOH online systems
- ENGAS
- DMS
- Fixed Assets and INVENTORY
- HOMIS
- EMR
- All Computer systems in the hospital

IX. REPEALING CLAUSE

Provisions from previous issuance that are inconsistent or contrary to the provisions of this Memorandum Order are hereby rescinded and modified accordingly.

X. SEPARABILITY

If any provision of this Memorandum Order is declared invalid, the other provisions not affected thereby shall remain valid and subsisting.

Republic of the Philippines
Department of Health
Center for Health Development Davao Region
SOUTHERN PHILIPPINES MEDICAL CENTER
JP Laurel Avenue, Bajada, Davao City
Trunkline: 082-227-2731 Faxline: 082-221-7029

XI. ENFORCEMENT

Any employee found to have violated any guideline and policy may be subject to disciplinary action as authorized by SPMC in accordance with SPMC disciplinary policies, procedures, and codes of conduct, up to and including termination of employment.

XII. EFFECTIVITY

This order shall take effect immediately.

LEOPOLDO J. VEGA, MD, FPCS, FPATACSI, MBA-H
Medical Center Chief