	OSPITAL NG PARAÑAQUE		Document Code: **OSPAR-ADM-IT -004**
			Issue Date:
ADMINISTRATIVE DIVISION APPROVAL MATRIX			Section / Department **INFORMATION TECHNOLOGY**
Policy Title: **Information Technology Administration Policy**			Page No.1of 2
Prepared By:	**Reviewed By:**		**Approved by:**
Michael Vallido OIC- IT Section	**Arnaldo S. Cortes, RN** Supervising Administrative Officer **Darius J. Sebastian, MD, MPH, PHSAE** **Hospital Administrator**		**Jefferson R. Pagsisihan, MD, MHM** Hospital Director

Objectives:

This policy provides guidelines for the administration of information technology assets and resources within the hospital.

Responsibility:

It shall be the responsibility of the IT section to report all problems and misuse of equipment's to the administrative department for proper action.

Procedures:

1. IT staff is responsible for the maintenance and management of all service agreements for the hospital technology. Any service requirements must first be approved by IT head. They will be responsible for maintaining adequate technology spare parts and other requirements.
2. A technology audit is to be conducted annually by IT section to ensure that all information technology policies are being adhered to.
3. Any unspecified technology administration requirements should be directed to IT staff
4. All software, including non-commercial software such as open source, freeware, etc. must be approved by the IT staff prior to the use or download of such software.
5. All purchases of software must be supported by warranty requirements and be compatible with the Ospar's server and/or hardware system.
6. Any changes from the above requirements must be authorized by IT staff.
7. In the event that open source or freeware software is required, approval from the IT section must be obtained prior to the download or use of such software.
8. All open source or freeware must be compatible with the hospital's hardware and software systems.
9. Any change from the above requirements must be authorized by IT section.
10. Any employee who notices misuse or improper use of equipment or software within the organization must inform his/her Reporting Manager(s) immediately.
11. Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software. Employees can request and/or the Management

			Document Code: **OSPAR-ADM-IT -004**
	OSPITAL NG PARAÑAQUE		Issue Date:
ADMINISTRATIVE DIVISION APPROVAL MATRIX			Section / Department **INFORMATION TECHNOLOGY**
Policy Title: **Information Technology Administration Policy**			Page No.2of 2
Prepared By:	**Reviewed By:**		**Approved by:**
	Arnaldo S. Cortes, RN Supervising Administrative Officer		
Michael Vallido OIC- IT Section	**Darius J. Sebastian, MD, MPH, PHSAE** **Hospital Administrator**		**Jefferson R. Pagsisihan, MD, MHM** Hospital Director

basis.

12. For major issues like PC replacement, non-working equipment, installation of application
    software and more, it is mandatory for all employees to inform the IT Dept.
13. Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet are prohibited,
14. downloading images, videos and documents unless required to official work
15. Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material unless explicitly required for office work.
16. Accessing pirated software, tools or data using the official network or systems
17. Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management Committee.
18. Engaging in any criminal or illegal activity or violating law
19. Invading privacy of coworkers.
20. Using the Internet for personal financial gain or for conducting personal business
21. Deliberately engaging in an online activity which hampers the safety & security of the data equipment and people involved.
22. Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.