OSPITAL NG PARAÑAQUE		Document Code: **OSPAR-ADM-IT -003**
		Issue Date:
ADMINISTRATIVE DIVISION APPROVAL MATRIX		Section / Department **INFORMATION TECHNOLOGY**
Policy Title: **POLICY ON SECURITY POLICY**		Page No.1of2
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

Objective:

This policy provides guidelines for the protection and use of information technology assets and resources within the hospital to ensure integrity, confidentiality and availability of data and assets.

Responsibilities:

1. It shall be the responsibility of the It section to ensure that all breach in the protocol of the IT security be identified and reported immediately.
2. It shall be the responsibility of the ensure that all equipment's are secured and free from damage and provided with antivirus.

Procedures:

1. For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through lock.
2. It will be the responsibility of It Section to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the IT staff immediately.
3. All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued a laptop, notepads, iPads, mobile phones. Each employee is required to use locks, passwords, and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.
4. In the event of loss or damage, the administrative office will assess the security measures undertaken to determine if the employee will be responsible for the loss or damage.
5. All laptop, notepads, iPadswhen kept at the office desk is to be secured lock provided by the IT staff.
6. It is the responsibility of IT staff to ensure that data back-ups are conducted every month and the backed-up data is kept in the hospital repository.
7. All technology that has internet access must have anti-virus software installed. It is the responsibility of IT staff to install all anti-virus software and ensure that this software remains up to date on all technology used by the hospital.
8. All information used within the hospital is to adhere to the privacy laws and the hospital's confidentiality requirements. Any employee breaching this will have appropriate sanction as determined by the Hospital Administration.

9. Every employee will be issued with a unique identification code to access the Technology and will be required to set a password for access every use.
10. Each password is to be determined by the staff to be consolidated by the IT staff and is not to be shared with any employee within the hospital.
11. Where an employee forgets the password or is 'locked out' after three attempts, IT STAFF is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.
12. Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.
13. Internet is a paid resource and therefore shall be used only for office work.
14. The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
15. The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received.
16. Username and password for a new employee must be requested by the HR Dept.
17. Sharing the Username and Password with another employee, visitor or guest user is prohibited.
18. Any password security breach must be notified to the IT Dept. immediately.
19. Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.
20. Lock your monitor screen, log out or turn off your computer when not at desk.
21. Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.
22. Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.
23. Not to connect USB memory sticks from an untrusted or unknown source to Ospar's equipment.