

Johns Hopkins Bayview Medical Center

GENERAL CLINICAL RESEARCH CENTER

Security of the Local Area Network

Policy No: 121

Original Date: 101997

Previous Date: none

Rev. Date: 05/2007

Purpose: To outline security mechanisms for the GCRC Local Area Network (LAN).

Procedure:

1. Software installation, alteration and deletion on the GCRC LAN are the responsibility of the GCRC Informatics Manager. The GCRC purchased software products are maintained in a locked cabinet on the GCRC.
2. Staff must adhere to all copyright laws included in the terms of software licenses. Software downloaded into any GCRC computer must have a valid license or an appropriate shareware agreement. Staff who are unsure of the status of a software product must contact the Informatics Manager before downloading or installing individual computer workstations to preserve the integrity of the GCRC network.
3. The LAN server room remains locked when not in use. Keys are held by the Informatics Core Staff, and the GCRC Administrative Manager. Room access is allowed to individuals who are skilled in server maintenance and functions.
4. Computer passwords are confidential. In the event that a password is deemed unsecured, it is the staff member's responsibility to have the password changed. The Informatics Manager has the authority to deny access to any user until the issue is resolved.
5. Computer access levels rights are assigned based on the individual's computer skills, the "need to know" principle, and the nature of her/his work. Access levels ("read only", "modify" and "full control") are determined by the GCRC administrative team and the Informatics Core.

Reviewer(s):

GCRC Informatics Manager

GCRC Charge Nurse

GCRC PCM

Pamela Ouyang, MD
Program Director, GCRC

Cynthia Walters, RN, MS, CNA
Senior Director of Nursing, JHBMC