Good Samaritan Health and Wellness Center

Policies and Procedures

Subject: Physical Security of Computers	Policy #: 4.9.14
Prepared by: John M. Hilliard	Effective Date: 07.21.16
Approved by: Board	Revision Date:

PURPOSE

Good Samaritan Health and Wellness Center has adopted a set of procedures and measures to prevent and prohibit unauthorized access or damage to facilities/computers that contain information systems.

SCOPE

This policy governs access to server rooms, wiring closets, communications closets and any other **Good Samaritan Health and Wellness Center** networking or computing equipment.

POLICY

The I.T. Department has developed procedures to protect **Good Samaritan Health and Wellness Center** computer assets from both environmental (water, heat) and human threats. These procedures include:

- Limiting physical access to the servers and network infrastructure equipment whenever possible. The **Good Samaritan Health and Wellness Center** server equipment is stored in an area with restricted access.
- Network and server equipment should be stored at a minimum of at least 6 inches off the floor whenever possible to reduce the possibility of water intrusion.
- Network/wiring closets should remain locked when unattended. Locks should allow only authorized staff access.
- The I.T Department maintains a list of staff and contractors that are considered authorized for access.
- Server rooms should remain in “non-public” areas with limited access and should not have direct exposure to external windows or doors.
- Desktop PCs shall be installed in secure areas that are locked after normal business hours or while unattended.

- Server equipment should use uninterrupted power supply (UPS) units to condition electricity quality and to provide electrical coverage in the event of a power outage.

PROCEDURE

- The I.T Department will review, and revise if necessary, the list of staff members authorized to access restricted areas.
- The list of staff members authorized to access the restricted areas will be prominently posted near the entrance of the restricted area(s).
- I.T will provide on-going training or announcements to remind authorized, as well as some unauthorized, staff members of this requirement. Additionally, this reminder will be a component presented at Security Committee meetings.
- Physical Security will be included in the annual security review.
- Restricted areas will be clearly marked as such.

VIOLATION REPORTING

Any observed/suspected violations of this policy should be immediately reported to the Information Security Officer.