**Good Samaritan Health and Wellness Center**
Policies and Procedures

| | |
|---|---|
| Subject: Physical Access | Policy #: 4.9.5 |
| Prepared by: John Hilliard | Revision # 1 |
| Approved By: Board of Directors | Effective Date: 04/22/2016 |

# 4.9.5 Physical Access

**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 that contain agency 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. The communication equipment is secured in "non-public" areas of the site.
- 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. All others must be escorted by a member of the I.T. staff during 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 in I.T. Departmental meetings at least twice per year.
- Restricted areas will be clearly marked as such.

## VIOLATION REPORTING

Any observed misuse or violation of this policy should be immediately reported to one of the following persons:

- Executive Director,
- Chief Financial Officer,
- Security Officer

## DEFINITIONS

Authorized staff – In general terms this is staff with roles that would require access to the restricted areas. Examples would include I.T. staff, Operations staff and Leadership Team members.

## SUPPORTING REFERENCES

Internet Security Forum (2007), The Standard of Good Practice for Information Security, *Critical Business Applications* (CB 3.1, CB 3.3), *Computer Installations* (CI 2.8, CI 4.1), *Security Management* (SM 4.5), *Networks* (NW 3.4), *End User Environment* (UE 6.4).

The Joint Commission Standards (2009), *Maintain Security & Integrity of Health Information* (IM 02.01.03).