General Policy F.3 **PORTABLE COMPUTER[S]**

Catholic Charities has adopted this Portable Computer Policy to comply with HIPAA and the regulations requirement to protect the security of electronic health information, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Catholic Charities who use laptop, notebook, or other portable computers must be familiar with the policy. Demonstrated competence in the requirements of the policy is an important part of every Catholic Charities employee's responsibilities.

Assumptions:

- Portable computers pose a significant security risk because they may contain confidential patient information and, being portable, are more at risk for loss, theft, or other unauthorized access than the facility's less easily movable computers.

- Portable computers may be more vulnerable to viruses and other such threats because the Employee may not regularly use virus protection software and other electronic safeguards the way the facility's Director of Health Information Management does on the facility's network.

- Portable computer use is more difficult for the facility to audit; thus security breaches may be more difficult to identify and correct.

Procedures:

Officers, agents, employees, contractors, and others using portable computers Employees must read, understand, and comply with this policy.

No person may use a personal computer for Catholic Charities' business purposes without the authorization of the Program Director. No Employee may, for any purpose, download, maintain, or transmit, confidential patient or other information on a personal computer without the written authorization of the Program Director.

Catholic Charities has issued the following computer equipment to you for the uses for which you have been specifically trained. The hardware, software, all related components, and data are the property of Catholic Charities and must be safeguarded and be returned upon request and upon termination of your employment. Your responsibility for the initial equipment extends to the equipment below and/or any exchanged or additional equipment Catholic Charities may issue you during your employment.

EQUIPMENT	SERIAL NUMBER	FACILITY ASSET NUMBER

The Employee agrees to use the equipment solely for Catholic Charities' business purposes. The Employee further understands:

- Dial in functions are restricted to dialing into Catholic Charities.
- Employee is not permitted to dial into any other unauthorized services, Internet service providers, or any other Internet access or to use the dial-up capabilities in any other manner than as instructed.
- Computers, associated equipment, and software are for business use only, not for the personal use of the Employee or any other person or entity.
- Employees will not download any software onto the computer except as loaded by authorized staff.
- Employees will not insert any disks, CDs, portable drives, or other media into the computer without the express authorization of the IS Administrator.
- Employees must use only batteries and power cables provided by Catholic Charities and may not, for example, use their car's adaptor power sources unless otherwise authorized.
- Employees will not connect any additional peripherals (keyboards, printers, modems, etc.) without the express authorization of the IS Administrator..
- Employees are responsible for securing the unit, all associated equipment, and all data, within their homes, cars, and other locations as instructed in the training provided.

- Employees will use the cable provided to lock equipment to immovable objects except when transporting the equipment.

- Employees may not leave mobile computer units unattended unless they are in a secured location.

- Employees should not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.

- Employees must place portable computers and associated equipment in their proper carrying cases when transporting them. The case must display the Employee's name and identify the facility.

- Employees must not alter the serial numbers and asset numbers of the equipment in any way.

- Employees will not permit anyone else to use the computer for any purpose, including, but not limited to, the Employee's family and/or associates, patients, patient families, or unauthorized officers, employees, and agents of Catholic Charities.

- Employees must not share their passwords with any other person and must safeguard their passwords and may not write them down so that an unauthorized person can obtain them.

- Employees must report any breach of password security immediately to the system administrator or Director of Health Information Management.

- Employees must maintain patient confidentiality when using the computers, as specified in Catholic Charities' Workstation Policy. The screen must be protected from viewing by unauthorized personnel, and Employees must properly log out and turn off the computer when it is not in use.

- Employees must *immediately* report any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the system administrator and Director of Health Information Management.

Enforcement:

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment in accordance with the facility's Sanction Policy.

_____ _____

Employee' Signature **Date**

_____ _____

Updated: February 2007

Employee's Title **Program**

Updated: February 2007