6Gx53-9.005 CONTROLLING ACCESS TO INFORMATION AND SYSTEMS:

A. Managing Access Control Standards

Access control standards for information systems will be established by management and should incorporate the need to balance restrictions to prevent unauthorized access with the need to provide unhindered access to meet business needs.

B. Managing User Access

Access to all systems must be authorized by the owner of the system and such access, including the appropriate access rights (or privileges) must be documented. Such documentation is to be regarded as confidential and safeguarded accordingly.

C. Securing Unattended Workstations

Equipment is to be safeguarded appropriately – especially when left unattended. It is each individual user's responsibility to ensure the equipment is secured when unattended.

D. Managing Network Access Controls

Access to the resources on the network must be strictly controlled to prevent unauthorized access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

E. Controlling Access to Operating System Software

Access to operating system commands is to be restricted to those persons who are authorized to perform systems administration/management functions

F. Managing Passwords

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason.

G. Securing Against Unauthorized Physical Access

Physical access designated high security areas are to be controlled with strong identification and authentication techniques. Staff with authorization to enter such areas are to be provided with information on the potential security risks involved.

H. Monitoring System Access and Use

Access to information systems is to be logged and monitored to identify potential misuse of systems or information.

I. Controlling Remote User Access

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques.

Statutory Authority**:** Florida Statutes 1001.32, 1001.41, 1001.42, 1001.43

Laws Implemented:

Adopted: September 21, 2004

Amended: