6Gx53-9.006 PROCESSING INFORMATION AND DOCUMENTS:

A. Accessing your Network Remotely

Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

B. Appointing System Administrators

The organization's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day-to-day running and security of the systems.

C. Administrating Systems

System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the organization. In addition, they must be knowledgeable with the range of Information Security risks, which need to be managed.

D. Controlling Data Distribution

For authorized personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy.

E. Managing System Operations and System Administration

The organization's systems must be operated and administered using procedures in a manner, which is both efficient but also effective in protecting the organization's information securely.

F. Monitoring Error Logs

Error logs must be properly reviewed and managed by qualified staff.

G. Monitoring Operational Audit Logs

Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system.

H. Transferring and Exchanging Data

Sensitive or confidential data/information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques.

I. Staff / Student Information

Student and Staff contact information is to be classified as confidential and secured accordingly. This information may only be updated by authorized personnel.

J. Backup and Recovery of Information

Information system owners must ensure that adequate back up and system recovery procedures are in place.

K. Using Encryption Techniques

Where appropriate, sensitive or confidential information or data should be transmitted in encrypted form. Prior to transmission, consideration must be given to the procedures to be used between the sending and recipient parties and any possible legal issues related to using encryption techniques.

L. Sharing Information

Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and organizational duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organization and to external parties.

M. Sending Information to Third Parties

Prior to sending information to third parties, not only must the intended recipient be authorized to receive such information, but the third party recipient must sign and return a confidentiality agreement to continue to assure the confidentiality and integrity of the information.

N. Fire Risks to Your Information

All data and information must be protected from the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded.

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

Laws Implemented:

Adopted: September 21, 2004

Amended: