TITLE: INFORMATION SECURITY

AUTHORITY:

> **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
> **Gramm-Leach-Bliley Act of 1999 (GLB)**
> **Sarbanes-Oxley Act of 2002 (SOX)**
> **Fair and Accurate Credit Transactions Act (FACTA)**
> **Family Educational Rights and Privacy Act (FERPA)**
> **Florida Statutes 282.318, 817.568, 1001.02, 1010.01, 1012.81**
> **State Board of Education Rules 6A-14.047, 6A-14.072**
> **International Organization for Standardization (ISO) 17799**

POLICY:

The purpose of this policy is to protect the College's information assets[1] from all threats, whether internal or external, deliberate or accidental and to ensure operational continuity by preventing breaches of security.

1. The College will use all reasonably practicable measures to ensure that information will be protected against unauthorized access.

2. The College will designate an information security manager who shall administer the security program of the College for its data and information technology resources.

3. Confidentiality of information will be assured to the extent required by applicable Florida and Federal law.

4. Integrity of information will be maintained.

5. Regulatory and legislative requirements will be met.

6. The College will conduct, and periodically update, a comprehensive risk analysis to determine the security threats to the data and information technology resources as needed.

7. Operational continuity plans will be produced, maintained and tested as needed.

8. College requirements for availability of information and information systems will be met.

TITLE: INFORMATION SECURITY

POLICY:

9. All College administrators will be directly responsible for implementing the Policy within their areas of responsibility, and for adherence by their staff.

10. Students, faculty and staff will report breaches of information security, actual or suspected**,** to any College administrator who will immediately escalate the incident to the College's designated Security Manager.

11. Breaches of the security policy will be investigated and handled in accordance with the College's disciplinary procedures.

Notes
[1] Information assets take many forms and include:
  - data stored on computers,
  - data transmitted across networks,
  - data printed or written on paper,
  - data sent by fax,
  - data stored on tape, CDs, DVDs and other removable computer data storage devices, or
  - informational representations spoken in conversations or over the telephone.