1.0 Purpose

Florida Gateway College (FGC) is steadily becoming more dependent on its computer-based information systems. Implementation of more sophisticated technologies implies better service-levels and increasing automation of operational and managerial procedures. Consequently, the College becomes more vulnerable to the unplanned interruption and corruption of Information Technology resources.

Protection of these resources from deliberate and/or accidental unauthorized access, use or modification is a major concern. Security of resources depends on some combination of access control measures, for which certain users possess keys. No combination provides absolute security. Ultimately, the level of security provided at any particular installation must result from a conscious decision weighing the trade-offs between the perceived risk, the cost of reducing that risk and the associated benefit from the risk reduction. The policy identifies the responsibilities of College organizational units with respect to these issues.

2.0 Scope

This Policy applies to all personnel at FGC.

Policy 6Hx12:12-26
3.0 Statement

The Executive Director/CIO, Information Technology is responsible for providing the means for accomplishing physical and logical security for the hardware, software and data under the direct control of his/her department.

All personnel are responsible for providing physical and logical security for Information Technology resources under their direct control. In this context, each College organizational unit (including Information Technology) as well as their sub-units, is considered a user.

Physical security includes but is not limited to:
- Controlling access to computer hardware.
- Preventing service interruptions (power, hardware failure).
- Planning for disaster and other contingencies.

Logical security includes but is not limited to:
- Controlling access to and use of software and data.
- Recovering data, transmissions and software.
- Archiving data, software and documentation.
The Information Security Officer (ISO) with the support of the Executive Director/CIO, Information Technology will coordinate ongoing efforts to identify security issues, develop and distribute standards and procedures, and implement both immediate and long range security and control means and strategies. Upon request, consultation will be provided, to personnel for areas under their direct control.

Physical and logical security status will be monitored, and violations will be reported to the appropriate level of authority.

History: Adopted: 11/11/09; Effective: 11/11/09