

SEMINOLE COUNTY GOVERNMENT AGENDA MEMORANDUM

SUBJECT: Information Security Policy

DEPARTMENT: Information Technologies DIVISION: Information Services

AUTHORIZED BY: Chris Grasso CONTACT: Kim Patterson EXT. x1100

Agenda Date <u>2/11/03</u>	Regular <input type="checkbox"/>	Consent <input checked="" type="checkbox"/>	Work Session <input type="checkbox"/>	Briefing <input type="checkbox"/>
	Public Hearing - 1:30 <input type="checkbox"/>		Public Hearing - 7:00 <input type="checkbox"/>	

MOTION/RECOMMENDATION:

Adopt resolution establishing Information Security Policy for Seminole County Government.

BACKGROUND:

The purpose of the Information Security Policy is to ensure that information and information systems are appropriately safeguarded. To date, the County's existing internal procedures and processes have been adequate to protect the assets of the County, but it is necessary to formalize this policy.

The approval of the Information Security Policy establishes that the County Manager shall approve and enforce the Information Security Guidelines. The Information Technologies Director or designee shall serve as the primary position to provide direction and technical expertise to ensure the protection of Seminole County's information.

The policy impacts not only computers and facilities, but also the people, processes, environment and technologies under the Board of County Commissioners. Supervisors, managers and directors will be held directly responsible for the implementation of the Guidelines and adherence by their staff. Additionally, employees will be held accountable for their compliance to the Policy and Guidelines.

The Information Security Policy will enable us to safeguard the assets of the County and serve as a benchmark to continually improve the state of our security.

Reviewed by:	<u>[Signature]</u>
Co Atty:	<u>[Signature]</u>
DFS:	<u> </u>
Other:	<u> </u>
DCM:	<u>SS</u>
CM:	<u>[Signature]</u>
File No.:	<u>CITR1</u>

THE FOLLOWING RESOLUTION WAS ADOPTED BY THE BOARD OF COUNTY COMMISSIONERS OF SEMINOLE COUNTY, FLORIDA, AT THEIR REGULARLY SCHEDULED MEETING ON THE _____ DAY OF _____, 2003.

WHEREAS, the Board of County Commissioners for the reasons stated hereafter believes it to be in the best interests of the citizens of Seminole County and the public in general to adopt an overarching Information Security Policy for Seminole County Government (the "Policy") and the guidelines and procedures to be promulgated thereunder; and

WHEREAS, the Policy, attendant guidelines and procedures are intended to apply to Seminole County Government employees under the Board of County Commissioners and third parties having access to internal County networks, operating systems, facilities, software, and hardware that is owned, leased, or managed by the Board; and

WHEREAS, the Policy is being adopted for the purpose of restricting access to and safeguarding the integrity of sensitive security measures designed to control and protect public access and availability of public documents and official records, as required in Section 119.07(3)(o), Florida Statutes and secondly, to fulfill the County's obligation under Section 119.085, Florida Statutes to protect the contents of public records from unauthorized access or alteration and to prevent disclosure or modification of such information therein which is exempt from disclosure under the public records laws of this State; and

WHEREAS, "information security," encompasses not only computer security and physical security of facilities but of necessity, also involves managing risks to information in all forms by establishing effective, efficient, and cost-wise security capabilities throughout the infrastructure that facilitates its use including not only the computers and facilities, but also the people, processes, environment, and technologies (data and voice networks in addition to computers); and

WHEREAS, an information security program is only effective when consideration for people and processes are integrated with environmental and technical control capabilities to deliver information security as opposed to security mechanisms focused only on physical security or technology that invariably experience the same problems over and over; and

WHEREAS, information and information systems are valuable assets to Seminole County Government, and the County relies on its information and information systems as a crucial and integral part of providing essential services including meeting its legal and moral responsibility to its constituents for balancing the need for public access to government records while ensuring the integrity of information, the confidentiality of private information, and the availability of their information and information systems; and

WHEREAS, the ultimate goal of a governmental organization's Information Security Program is to establish enterprise-wide security capabilities that will enable it to safely utilize information technology to provide faster, accurate service and better on-line access to constituents; protect the organization from potential losses and improve the stability of systems; and minimize legal and regulatory liabilities; and

WHEREAS, the perspective as described above, combined with the concepts presented in ISO/IEC 17799 as defined in the Policy provides the foundation from which the Policy and Guidelines are to be developed:

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF SEMINOLE COUNTY THAT:

(1) The forgoing recitals comprise an integral part of the findings and determinations underlying the adoption of this Resolution.

(2) The Information Security Policy shall be as stated in the following paragraphs of this Resolution.

(3) The Board of County Commissioners hereby adopts the Information Security Policy to ensure that information and information systems are appropriately protected from a variety of threats, both natural and manmade. The Board's intent is to ensure that information and systems are protected at a level commensurate with their value and sensitivity and that citizens can access public records as required by law. Security controls shall be employed on all media where information is stored, the systems that process it, and infrastructure components that facilitate its transmission. Controls shall be in place to positively identify individuals that have access to the Seminole County Government network or systems and to restrict access to information based on the concept of least privilege—that is, users are provided access only to the systems, services, and information needed in the performance of their official duties, and no more—while allowing unfettered access for the public to view and download (but not alter) public records. To this end, Seminole County Government will allocate sufficient time and resources to ensure the protection of its information.

(4) Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know what constitutes acceptable use of Seminole County Government systems, to know the guidelines, and to conduct their activities accordingly. All employees and third-party vendors shall receive training and supporting reference materials to allow them to properly protect Seminole County Government information assets before they are granted access. Security awareness training shall be provided at regular intervals to ensure they maintain the desired level of proficiency.

(5) The purpose of the Information Security Policy and Guidelines are first and foremost to effectively and efficiently manage the risks to Seminole County Government's information assets from all types of threats, whether internal or external,

deliberate, or accidental. Information Security is critical to the organization's survival. Beyond this primary objective is also the goal of utilizing information security as an enabler for proper information sharing and the benefits of a strong program, such as increased ease of administration, reduced complexity of the security architecture, transparency to users, and reduced effort on the part of users, not to mention enhanced security.

As it pertains to the primary goal of protection, the Board of Commissioners has established these overriding objectives:

- (a) Information will be protected against unauthorized access, while providing for public access as required by law;
 - (b) Confidentiality of information will be assured;
 - (c) *Integrity of Information will be maintained;*
 - (d) Users will be held accountable for their activities;
 - (e) Physical, logical, environmental and communications security will be maintained;
 - (f) Legal, regulatory, and contractual requirements will be met;
 - (g) Business continuity plans will be produced, maintained, and tested,
- and
- (h) Information security awareness and training will be provided to all staff.

(6) The need to protect information must be balanced with the need for open government, as established in The Public Records Act (Chapter 119, Florida Statutes). This act provides for public access to government information in all forms (written and electronic), but also provides for exemptions to protect certain private or confidential information. Section 119.085 requires custodians of electronically stored public documents to provide safeguards against document tampering and unauthorized access to information deemed exempt from public disclosure. Lastly, Section 119.07(3)(o) provides authority for the exemption from public disclosure of those computer applications related to protecting the internal security and integrity of a public agency's data information systems. Seminole County employees will comply with these statutes and the exemptions specified by the Florida Legislature, as defined in the *Florida Attorney General's Government-in-the-Sunshine Manual*. Annual reviews of the risks to the County's information and information systems and compliance with this Policy and Guidelines shall be performed and reported to the Board to ensure appropriate visibility exists for the protection being applied to our information and information systems.

(7) Non-compliance with this Policy by Seminole County employees and systems users is a serious matter and will be dealt with accordingly on a case-by-case basis. Depending on severity of violations and applicable legal statutes, consequences could result in removal of access rights and special system privileges, removal of system access, or, for County employees, disciplinary action to include potential termination of employment. In severe cases of fraud or breach of privacy laws, legal action may be taken.

(8) The Board of County Commissioners bears ultimate authority and responsibility for Seminole County Government's Information Security. As such, the Board has established this Policy and directs Seminole County Government personnel to implement the Information Security Policy, as follows:

(a) The County Manager shall approve and enforce all Information Security Guidelines that have county-wide scope.

(b) The Information Technologies Director or designee shall be appointed by the County Manager as the Information Security Officer (ISO) to provide the direction and technical expertise to ensure that Seminole County Government's information is properly protected.

(c) All Seminole County Government Directors, Managers, Program Managers, and Supervisors are directly responsible for implementing the Information Security Policy and Guidelines within their areas of responsibility, and for adherence by their staff.

(d) It is the responsibility of each employee to adhere to the Information Security Policy and Guidelines and to ensure that any vendors or visitors that they sponsor also comply.

(9) The ISO shall periodically review the program for effectiveness, and will report compliance findings to the Board of County Commissioners on an annual basis.

(10) The Resolution shall take effect upon its adoption and shall supercede all prior resolutions or sections thereof that are in conflict with this Resolution.

DATED this _____ day of _____, 2003.

Board of County Commissioners
Seminole County, Florida

By: _____
DARYL G. MCLAIN, Chairman