SECTION 26. INFORMATION SERVICES DEPARTMENT

26.5 INFORMATION SECURITY

A. PURPOSE.

(1) The purpose of the Information Security Policy and Guidelines is 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.

(2) Security is critical to the organization's survival. 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.

B. OBJECTIVES.

(1) Seminole County Government 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.

(2) 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.

C. TRAINING.

(1) Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems.

(2) 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.

(3) 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.

(4) Security awareness training shall be provided at regular intervals to ensure they maintain the desired level of proficiency.

D. INFORMATION PROTECTION/COMPLIANCE.

(1) Must be balanced with the need for open government, as established in The Public Records Act (Chapter 119, Florida Statutes).

(2) Provides for public access to government information in all forms (written and electronic).

(3) Provides for exemptions to protect certain private or confidential information.

(4) Requires custodians of electronically stored public documents to provide safeguards against document tampering and unauthorized access to information deemed exempt from public disclosure.

(5) 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.

(6) Annual reviews of the risks to the County's information and information systems and compliance with this Policy shall be performed and reported to the Board of County Commissioners (BCC) to ensure appropriate visibility exists for the protection being applied to our information and information systems.

E. NON-COMPLIANCE. Non-compliance with this Policy by Seminole County employees and system 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.

F. RESPONSIBILITY. 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:

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

(2) The Information Services Department 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.

(3) 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.

(4) 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.

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

G. AUTHORITY. Public Records Act, Chapter 119, Florida Statutes
Resolution 2003-R-36 adopted February 11, 2003
Resolution 2007-R-42 adopted March 13, 2007
Resolution 2008-R-55 adopted February 12, 2008
Resolution 2010-R-26 adopted January 26, 2010
Resolution 2012-R-107 adopted June 12, 2012