CHAPTER 3

TECHNOLOGY ROLES AND RESPONSIBILITIES

PURPOSE:

Technology development and management is a repetitive process that must include active involvement and strong commitment from all parties: management, Department offices that use information technology, and the Office of Information Technology (OIT).

The purpose of this policy is to ensure the Florida Department of Transportation (FDOT) has:

(1) The best technology possible to support our business and strategic goals;

(2) Department personnel who are informed of, competent in, and capable of using technology to the greatest extent possible to enhance organizational effectiveness and efficiency; and

(3) The technological capacity to develop, maintain, and support our technology goals and objectives.

When filling vacancies, managers should seek to fill positions with individuals who have technology experience in addition to their specific job skills. These individuals shall work in conjunction with personnel from Transportation Technology (TT) to develop, maintain, and support the Department's technologies.

AUTHORITY:

Sections 20.23(4)(a) and 334.048(3), Florida Statutes (F.S.)

3.1 TRANSPORTATION TECHNOLOGY RESPONSIBILITIES AND ROLES

TT shall be responsible for:

(1) administration of the Department's information management and communications programs;

(2) providing staff to be highly trained in information management and technology;

(3) ensuring the integrity and safeguarding of the data within the systems of the Department's computers over which TT has control;

(4) the development and/or acquisition, maintenance and operational support of all Department mission critical applications (mission critical applications are those in which information, if lacking or inaccurate, will have an adverse effect on the performance and management of the Department);

(5) developing, publishing and distributing departmental procedures, directives, policy statements, rules, standards and guidelines for information resources;

(6) overseeing technology solutions developed and/or acquired by end-users to solve their particular business needs;

(7) providing consulting services to end-user offices on technology issues to make the most efficient use of the appropriate technology for a particular application;

(8) testing and certifying hardware and software for FDOT use;

(9) serving as coordinator for the distribution of hardware and software to the user community;

(10) establishing and directing quality assurance monitoring of all units in the functional area of information resources;

(11) ensuring the Department's technology solutions are integrated, as appropriate, to facilitate the sharing of this important agency asset;

(12) providing advice, council and guidance to those FDOT offices that are desirous of developing technology solutions within their office;

(13) providing training to end-users regarding the TT policies, procedures and best practices via classroom, computer based training, or other methods; and

(14) must adhere to ***F.A.C. 60-8, Accessible and Electronic Information Technology.***

3.2 END-USER ROLES

FDOT Offices' Responsibilities:

(1) shall use as their source of data, the data residing on the Department's mainframe and engineering/CADD computers, or available through the statewide Department network, unless there is a compelling reason to do

otherwise, such reason shall be documented and forwarded to the Chief Information Officer (CIO) via the IRR system;

(2) shall ensure the integrity of the data and systems as required by ***74-2, Florida Administrative Code***;

(3) shall forward a copy of the documentation of the technology solutions developed and/or acquired to the CIO to be made a part of the Department's technology solutions documentation;

(4) develop technology solutions using appropriate hardware and software;

(5) consult with and request assistance from TT;

(6) shall ensure critical infrastructure or high-risk systems design and documentation is safeguarded under **F.S. 119** as applicable. This includes system topology, Internet Protocol schema and address ranges, remote switch or hub sites and other records which might expose system vulnerabilities that would impact the mission of the Department or the public directly;

(7) must adhere to the system security plan and any risk or threat assessments;

(8) must adhere to ***F.A.C. 60-8, Accessible and Electronic Information Technology.***

TRAINING:

None Required.

FORMS:

None Required.