Transportation Technology Manual Definitions

Term	Abbreviation	Definition
Access		Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (Source: Rule 74-2.001, F.A.C.)
Access Control		The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). (Source: Rule 74-2.001, F.A.C.)
Access Point		A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network. (Source: Rule 74-2.001, F.A.C.)
Accountability		Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (Source: Rule 74-2.001, F.A.C.)
Active Directory	AD	A Microsoft service which is a central component of the Windows® operating system platform; a directory service provides a place to store information about network-based entities, such as applications, files, printers, and people. It provides a consistent way to name, describe, locate, access, manage, and secure information about these individual information resources; a directory service acts as the main switchboard of the network operating system. It is the central authority that manages the identities and brokers the relationships between these distributed information resources, enabling them to work together. Because a directory service supplies these fundamental network operating system functions, it must be tightly coupled with the management and security mechanisms of the operating system to ensure the integrity and privacy of the network. It also plays a critical role in the Department's ability to define and maintain the network infrastructure, perform system administration, and control the overall user experience of the department's information systems.

Active Directory Domain		A single security boundary of a Windows-based computer network. Active Directory is made up of one or more domains. On a standalone workstation, the domain is the computer itself. A domain can span more than one physical location. Every domain has its own security policies and security relationships with other domains. When multiple domains are connected by trust relationships and share a common schema, configuration, and global catalog, they constitute a domain tree. Multiple domain trees can be connected together to create a forest.
Active Directory Group		A Windows group that simplifies security by allowing access rights to be granted to a group of people rather than individuals.
Agency for Enterprise Information Technology – Office of Information Security, The	AEIT-OIS	Guides, coordinates, and assists state agencies in identifying threats to information assets and mitigating vulnerabilities, so effective security controls can be implemented.
Agency for State Technology	AST	Established in 2014 by the Florida legislature to develop and publish information technology policy for the management of the state's information technology resources.
Agency Worker		See **Worker**; **Workforce**.
Agency-Approved software		Software that has been reviewed and deemed acceptable by the agency for use with agency information technology resources.
Agency-Managed Device		A device that is not owned by the agency, but that is declared by the device owner and accepted by the agency to be compliant with agency standard configurations.
American Association of State Highway and Transportation Officials	AASHTO	A standards setting body which publishes specifications, test protocols and guidelines which are used in highway design and construction.
American Standard Code for Information Interchange	ASCII	The de facto world wide standard for the code numbers used by computers to represent all the upper and lower case Latin letters, numbers, punctuation, etc. There are 128 standard ASCII codes each of which can be represented by a 7 digit binary number: 0000000 through 1111111.
Anti-Malware Software		Software that detects and removes malicious software from a computer or network stream.
Application		A software program hosted by an information system. (Source: Rule 74-2.001, F.A.C.)
Application Components, Computer		Computer programs, executables and environmental components, and batch jobs necessary to provide the Department with a business application. Excludes COTS application code.

Application Development		Work that requires one or more of the following: (A) The creation of a new application system and the database structure belonging to that application, or the implementation and delivery of a commercial off-the-shelf (COTS) application system. (B) Significant changes to functionality or technical environment of an existing application system that renders the original application system obsolete, such as the retooling of a mainframe application to a Web application.
Application Development Life Cycle	ADLC	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (also known as System Development Life Cycle – SDLC). (Source: Rule 74-2.001, F.A.C.)
Application Development Team		The entire set of people responsible for planning, designing, developing, installing, and maintaining applications. The roles represented include project managers, analysts, computer programmers, database administrators, data administrators, system administrators, network administrators, etc. (Source: Rule 71A-1.002, F.A.C.)
Application Owner		The business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc. (Source: Rule 71A-1.002, F.A.C.)
Application Programming Interface	API	
Application Security Review		An evaluation of an application's security requirements and associated controls (planned or implemented) with the goal of determining if controls are sufficient to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources. (Source: Rule 71A-1.002, F.A.C.)
Application Services Bureau		The unit in OIT responsible for the following functional areas: (a) development and maintenance of statewide core application systems that support the primary business processes of the Department, including financial management and production management planning and operations; and (b) overall coordination of Internet and Intranet application development and activity. (Formerly **Business Systems Support Office**.)
Audit Logs		A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (Source: Rule 74-2.001, F.A.C.)

Authentication		The process of verifying that a user, process, or device is who or what it purports to be. Techniques for authentication fall into categories as follows: (a) Something the user knows, such as a password or PIN; (b) Something the user has, such as a smartcard or ATM card; and (c) Something that is part of the user, such as a fingerprint, voice pattern or retinal scan. (Source: Rule 74-2.001, F.A.C.)
Authentication Code		A code of up to eight (8) characters chosen by the user to uniquely identify the user when a password reset request is made. This code will only be established when a user-ID for a corporate account is issued. Additionally, the authentication code will not change or expire unless requested by the user in person or in writing.
Authorization		Access privileges granted to a user, program, or process or the act of granting those privileges. (Source: Rule 74-2.001, F.A.C.)
Automated Access Request Form	AARF	This system is used to automate computer security access requests, approvals, and authorizations.
Availability		Ensuring timely and reliable access to and use of information. (Source: Rule 74-2.001, F.A.C.)
Breach		Unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information. (Source: Rule 71A-1.002, F.A.C.)
Browser		The computer program or software application that allows a user to access and display Web documents.
Business Case	BC	Documentation providing the project request, risks, benefits and costs for the purpose of authorizing and prioritizing the project by FDOT executive management. The Business Case is developed by the Project Sponsor and stakeholders. The OIT Portfolio management team (Innotas Team) performs a quality assurance check of the business case for completeness prior to it being submitted to the CIO and Executive Management.
Business Case Team	BCT	A team consisting of stakeholders involved in development of the business case. This team provides the initial, level-of-effort estimate based on historical data and expert judgment.
Business Continuity Plan		A collection of procedures and information designed to keep an agency's critical operations running during a period of displacement or interruption of normal operations. (Source: Section 282.0041, Florida Statutes)
Business Systems Support Office	BSSO	No longer active. See **Application Services Bureau**.

Central Office	CO	Central Office
Chief Information Officer	CIO	Agency official responsible for: 1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information systems are acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) developing, maintaining, and facilitating the implementation of a sound and integrated information system architecture for the agency; and 3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. (Source: Rule 74-2.001, F.A.C.)
Code		A system of rules to convert information into another form or representation for communication through a channel or storage in a medium.
Commercial Off-the-Shelf Products	COTS	An item that is commercially available (leased, licensed, or sold) to the general public and which requires no special modification or maintenance over its life cycle because it is designed to be implemented without the need for extensive customization.
Communications Service Authorization and Billing System	CSAB	
Communications, Data Processing		Transmission of data via a combination of network hardware and software across the Department's local area and wide area network in support of data processing efforts (for example, file and print sharing, e-mail, database queries, etc.).
Compensating Security Control		A management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control that provides an equivalent or greater level of protection for an information system and the information processed, stored, or transmitted by that system. (Source: Rule 74-2.001, F.A.C.)
Complete Record		An electronic record that has been verified using a manual page count to ensure that the original hard copy's number of pages match the EDMS scanned copy's number of pages.
Complex Password		A password that is at least eight characters and is comprised of at least three of the following categories: uppercase English letters; lowercase English letters, numbers 0-9, and non-alphanumeric characters. (Source: Rule 71A-1.002, F.A.C.)
Comprehensive Risk Assessment		The risk analysis required to be conducted by agencies every three years, in accordance with Section 282.318, F.S. (Source: Rule 71A-1.002, F.A.C.)
Computer		An internally programmed, automatic device that performs data processing. (Source: Section 815.03, Florida Statutes)

Computer Aided Drafting and Design	CADD	The software and methods used to analyze, design and represent transportation facilities graphically. CADD facilitates the presentation of engineering data. Electronic engineering data and CADD comprise the department's engineering technology.
Computer Based Training	CBT	Training that is computer based.
Computer Security Access Request Form	CSAR	The form required to be completed in order to gain access to Department IT resources.
Computer Security Administration	CSA	Section of OIT. Enterprise Technology and Security Management is responsible for ensuring that FDOT assets are protected according to Florida statutes by coordinating and administering security policies, procedures, and standards. Compliance is ensured through security awareness training and security compliance assessment.
Computer Services		Providing a computer system or computer network to perform useful work. Includes, but is not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.
Computer Services Office	CSO	No longer active. Formerly an Office within OIT.
Computer System		A device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files. (Source: Section 815.03, Florida Statutes)
Computing Facility, Agency		Agency space containing fewer than a total of 10 physical or logical servers, but excluding single, logical-server installations that exclusively perform a utility function such as file and print servers. (Source: Section 282.0041, Florida Statutes)
Confidential Information and/or Confidential Data		Records that, pursuant to Florida’s public records laws or other controlling law, are exempt from public disclosure. (Source: Rule 74-2.001, F.A.C.)
Confidentiality		Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Source: Rule 74-2.001, F.A.C.)
Configuration Management		The detailed recording and updating of information that describes an enterprise’s hardware and software. Such information typically includes the versions and updates that have been applied to installed software packages as well as the locations and network addresses of hardware devices.

Consultant		A person who provides expert advice professionally. Consultant is the working title for those individuals that are paid through Staff Augmentation Contracts, sub-contracted through Vendors outside of the FDOTtostaff a project and respond to business objectives. (See also: **Staff Augment**)
Contaminant, Computer		Any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions, commonly called viruses or worms, which are self-replicating or self-propagating and which are designed to contaminate other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp or interfere with the normal operation of the computer, computer system, or computer network. (Source: Section 815.03, Florida Statutes)
Content		Any information displayed by either a static Web page or a Web application. Content includes information housed in applications that are imported or linked into the Web page or application, such as Word, Excel or PowerPoint documents.
Contingency Factor	CF	A factor applied to all estimates. The contingency factor covers unknowns within the defined scope of the business case or project. The contingency factor reduces over the life of the project. The amount of the contingency factor is not a set percentage for all projects, but is based on the risks and project specifications. All factors that led to the contingency factor will be documented.
Continuity of Operations Plan	COOP	The documented plan detailing how the agency will respond to incidents that could jeopardize the organization's core mission pursuant to Section 252.365, F.S. (Source: Rule 71A-1.002, F.A.C.)
CO-OIS PRODMOVE Group		An e-mail distribution group that contains OIT personnel responsible for the actual migration or moving of computer application components to various production environments.
Critical Information Resources		The resources determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have severe or catastrophic adverse effect. (Source: Rule 71A-1.002, F.A.C.)
Cryptography		The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (Source: Rule 74-2.001, F.A.C.)

Cryptography, Strong		The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Secure Hash Algorithm revision 1 (SHA-1) is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include Advanced Encryption Standard (AES) 128 bits, Triple Data Encryption Standard (TDES), minimum double-length keys, Rivest, Shamir and Adleman (RSA), 1024 bits and higher, Elliptic Curve Cryptography (ECC), 160 bits and higher, and ElGamal (1024 bits and higher). (Source: Rule 74-2.001, F.A.C.)
Custodian		Guardian or caretaker of an information resource, the holder of data, or the employee or organizational unit charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource. The custodian is normally a provider of services.
Data		Representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device. (Source: Section 815.03, Florida Statutes)
Data Center, Agency		Agency space containing 10 or more physical or logical servers. (Source: Section 282.0041, Florida Statutes)
Data Custodian		Usually the person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices. SeeCustodian.
Data Steward		A person responsible for the management of data elements (also known as critical data elements) - both the content and metadata.
Data Store		A collection of information organized so it can be accessed, managed, and updated. (Source: Rule 71A-1.002, F.A.C.)
Database Administration Group	DBA	Database Administration Group; this group is housed within Application Services of the Office of Information Technology. Also known as Application Services Operations Team, AsOps

Degaussing		A method of bulk erasing data from magnetic media. Degaussing demagnetizes the disk such that all data stored on the disk is permanently destroyed. (Source: Rule 71A-1.002, F.A.C.) Any degausser equal to the Garner Products HDTD-8200 degausser, issued to the Department's Districts, shall be used for this task. This type degausser renders magnetic media and devices inoperable after degaussing.
Delegates		Employees that have been given permission from a member of the OIT management team to carry out certain management team member responsibilities on their behalf.
Demilitarized Zone	DMZ	An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (Source: Rule 74-2.001, F.A.C.)
Department	FDOT	The Florida Department of Transportation.
Department Standard		An established criterion to achieve a desired level of quality, which impacts the operations of more than one office or district. Any deviation must be approved and documented as an exception and supported by sound judgment.
Derivative Works		Any and all computer programs in executable code or source code form developed or otherwise acquired by the licensee which are a modification of, enhancement to, derived from, or based upon the software.
Destruction		The highest level or ultimate form of sanitization. The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverization, shredding, melting, sanding, and chemical treatment.
Development Infrastructure		A technical environment that is used for design, development, and/or piloting of new technical capabilities or applications. The development infrastructure is separated logically or physically from the production and test infrastructures. (Source: Rule 71A-1.002, F.A.C.)
Directly Connect [To The Agency Internal Network]		A device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected. (Source: Rule 71A-1.002, F.A.C.)
Disaster Recovery Plan		See **Information Technology Disaster Recovery Plan**.
Disposal		The act of discarding media or devices from Department use in a manner short of destruction. FDOT Policy 350-090-005 Surplus Property Disposal defines the practices that shall be followed for the proper disposal of electronic media vice properties.

Distributed Application		An application utilizing a distributed computer system.
Distributed Computer System		Any multi-user computer system that can operate independent of the Department's mainframe computer.
District		For purposes of this procedure, the term, district, refers to the 7 geographical districts, Turnpike District, Central Office, Central Warehouse, Office of Toll Operations, and Motor Carrier Compliance.
District Application Coordinator		A district personnel resource from a district business area that is committed to project activities and ongoing communication and coordination between the Functional Application Coordinator, the District office in that business area and the Technology Service and Support Office.
District Information System Manager	DISM	No longer active. See **Technology Services and Support Manager**.
District/Office Intranet Server		The Intranet server owned and maintained by a district or user office which contains Intranet information supplied and managed by that district or user office. This server must be linked to the Primary Intranet Server.
Document Preparation		Also known as "Prepping." Those activities designed to prepare a document to be scanned. This includes tasks such as inventorying pages, unpacking, unfolding, unbinding fasteners (removing staples, paperclips, etc.), repairing damaged pages, smoothing out pages, rotating pages and inserting identifying materials such as separator sheets, and setting scanners for single or double sided copies.
Domain Name		A domain name is the keyword responding to a unique address on the Internet. Domain names are also known as Web addresses (example: myflorida.com). To use a particular domain name, that name must be registered with an authorized vendor.
EDMS Procedure, Local		This local EDMS procedure describes in detail the EDMS quality assurance (QA) and quality control (QC) requirements for an office within a business area, including specific requirements for operating scanning hardware, providing a quality control sampling methodology, and rescanning bad documents. See Topic No. 025-020-002, Standard Operating System, Sections 2 and 12. (See **Electronic Document Management System**.)
EDMS, Enterprise	EEDMS	The Department’s approved enterprise EDMS application (currently Hummingbird DM). (See **Electronic Document Management System**.)
EDMS, Independent		Any EDMS that is not part of the enterprise EDMS. (See **Electronic Document Management System**.)
EDMS, One-Location		An enterprise EDMS involving records being scanned exclusively for a single location or office. (See **Electronic Document Management System**.)

EDMS, Statewide		A statewide EDMS involves records being scanned at multiple locations throughout the state for a single business area such as Construction, Structures Maintenance, Survey and Mapping, Engineering and Design, etc. (See **Electronic Document Management System**.)
EIP Link		A link displayed on the EIP that points to an Information Asset. (See **Enterprise Information Portal**.)
EIP Link Request		A request submitted by an Asset Owner to have an Information Asset added to, changed, or removed from the EIP. (See **Enterprise Information Portal**.)
EIP Project Manager		We have an EIP but not an EIP Project Manager, though we have other managers. (See **Enterprise Information Portal**.)
Electronic Device		A device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a cellular telephone, tablet, or other portable device designed for and capable of communicating with or across a computer network and that is actually used for such purpose. (Source: Section 815.03, Florida Statutes)
Electronic Document Management System	EDMS	Software developed to manage the capture, storage, retrieval, security version control, distribution and overall administration of electronic documents.
Elevated Computer Security Access		Capability that is authorized and assigned to enable OIT personnel and contract workers working in OIT to approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources that are protected or restricted.
Encryption		Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. (Source: Rule 74-2.001, F.A.C.)
End Users		Users of Information Technology Resources.
Enhancement		A change to an application system (addition, change or deletion) that affects its functionality. Generally the change is discretionary. Examples include adding, deleting or changing a screen or batch input; changing input edits or calculations; creating a new report or table; adding fields or columns to an existing report or table; changing the process required to create a report; or changing a file format.
Enterprise Communications & Administrative Services	ECAS	No longer active. As part of the TSSO, the ECAS unit provided voice, data and video conferencing services as well as enterprise managed services to the Department.

Enterprise Data Steward		A job role that involves planning, implementing and managing the sourcing, use and maintenance of data assets in an organization. Data stewards enable an organization to take control and govern all the types and forms of data and their associated libraries or repositories.
Enterprise Information Portal	EIP	An internal FDOT website that provides, links to Information Assets including a search engine for Information Assets and internal documents as well as the ability to customize the portal page for different user groups and individuals. It is the internal equivalent of the general-purpose portal on the Web.
Enterprise Software		Enterprise software is computer software used to satisfy the needs of an organization rather than individual users. Enterprise software is an integral part of a computer-based information system. The main goal behind enterprise software is to improve enterprise productivity and efficiency through business logic support functionality.
Enterprise System Owner		The Central Office SMS or traditional SES manager responsible for the function supported by the statewide EDMS (e.g., Construction EDMS or Engineering and Design EDMS).
Enterprise Technology Services and Support	ETSS	No longer active. A part of the TSSO, provided a range of enterprise IT security services to help ensure that information technology resources were reliable, available, and protected.
Erasure		Process intended to render magnetically stored information or data irretrievable by normal means.
Event		An observable occurrence in a system or network. (Source: Section 282.0041, Florida Statutes)
Exception to Standard		Not conforming to an existing standard.
Executable Code		The computer code for the software in a form that is intended to be directly executed by a computer.
Executive IT Governance Board	EITGB	Comprised of the Assistant Secretary for Finance and Administration (Chair), the Assistant Secretary for Intermodal Systems Development, and the Assistant Secretary for Transportation Policy. The Chief Information Officer (CIO) serves as a non-voting member of the Council.
Exempt Information		Information an agency is not required to disclose under Section 119.07(1), F.S., but which the agency is not necessarily prohibited from disclosing in all circumstances. (Source: Rule 71A-1.002, F.A.C.)

Extranet		A computer network that allows controlled access from the outside, for specific business or educational purposes. In a business-to-business context, an extranet can be viewed as an extension of an organization's intranet that is extended to users outside the organization, usually partners, vendors and suppliers, in isolation from all other Internet users. An extranet is similar to a DMZ in that it provides access to needed services for channel partners, without granting access to an organization's entire network. (Compare to **Intranet**.)
FDOT Enterprise Library	FEL	
FDOT Service Desk		An application which allows Department customers to open a new request for service (ticket) or check the status of an existing request for service.
File Transfer Protocol	FTP	A common method of moving files over a network or the Internet.
Financial Instrument		Any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security. (Source: Section 815.03, Florida Statutes)
Firewall		The primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure.
Fiscal Year End	FYE	The closeout of the current fiscal year's financial transactions and the opening of the next fiscal year's financial transactions.
Florida Administrative Code	FAC	The Florida Administrative Code is the official compilation of the administrative rules and regulations of state agencies.
Florida Statutes	FS	The Florida Statutes are the codified, statutory laws of Florida.
Forest		The Active Directory framework that holds the objects can be viewed at a number of levels. The domain, trees, and forest are the logical divisions in an Active Directory network. At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

Functional Application Coordinator	FAC	A dedicated resource from the functional office assigned to serve as liaison between the Office of Information Technology and the functional office. The Functional Application Coordinator may act as an agent for the application owner and is responsible and accountable for: (1) coordinating with the appropriate functional staff to clarify requests, (2) establishing priorities when multiple requests exist, (3) coordinating the timely and complete functional acceptance testing, and (4) providing approvals to progress any work from one phase to another, including final approval to move application modifications to the production environment. In cases where there are three or more closely related, interdependent applications that process together as a suite, A FAC must be appointed to act as the overall coordinator for the applications within the suite. The suite FAC is responsible for coordinating and communicating with the individual FACs and the Application Services Bureau on issues that affect the overall suite of applications. This includes coordination and prioritization of service requests among the functional application coordinators within the suite, production support, suite-wide maintenance releases, user notification, and system integration testing coordination.
Functional Experts		Employees who are experts in specific business processes within a business area of the Department and who participate in application systems development, enhancement and/or maintenance project activities pertaining to those business processes. Functional experts are accountable to the Functional Area Coordinator (FAC) and ensure the business area's process requirements are met.
Functional Office		The functional area within the Department, including both the central office and District counterparts, whose activities are supported by an OIT application.
Functional Review		A review conducted to ensure that a proposed information asset has value to the Department and is appropriate for inclusion in the EIP.
Functional Steering Committee		A committee comprised of business area managers with the authority to make recommendations or decisions that affect the functional area they represent.

Generic Account		The ISM has defined this type of account as being tied to a human(s) (example: training room accounts) used to log on 'interactively' (a key difference comparable to service accounts) and for a specific amount of time (e.g. DB2CNTL account). FDOT shall keep accurate logs of the actions taken by these accounts (when and from where, etc.) and shall be tracked by ownership/responsible person in the AARF system. At a minimum, actions shall be logged by the FDOT Log Management software. Internal logging by specific applications will be subject to the business rules applied to each application as described in the System Security Plan. These accounts shall be tied to a specifically identified machine or machines consistent with their requested authorization documented in the Department's AARF system. Example: It is unacceptable for a generic account assigned to a training room to be used anywhere except the training room machines for which the account was requested and approved.
Geographic Information Systems	GIS	An organized collection of computer hardware, software, and geographic data designed to efficiently capture, store, update, manipulate, analyze and display all forms of geographically referenced information.
Global Positioning System	GPS	Both survey Grade and Resource equipment.
Graphical User Interface	GUI	A visual way of interacting with computer using items such as windows, icons, and menus, used by most modern operating systems.
Hardware		Information technology equipment designed for the automated storage, manipulation, and retrieval of data by electronic or mechanical means, or both, and includes, but is not limited to, central processing units, front-end processing units, including mini-processors and micro-processors, and related peripheral equipment such as data storage devices, document scanners, data entry, terminal controllers and data terminal equipment, computer-related word processing systems, and equipment and systems for computer networks.
High Availability and Disaster Recovery	HADR	High availability is the measurement of a system's ability to remain accessable in the event of a sysytem component failure. Disaster recovery is the process by which a system is restored to a previous acceptable state.
HyperText Markup Language	HTML	The coding language used to create HyperText documents for use on the World Wide Web. HTML looks a lot like old-fashioned typesetting code, where you surround a block of text with codes that indicate how it should appear. Additionally, in HTML you can specify that a block of text or a word is linked to another file on the Internet. HTML files are meant to be viewed using a World Wide Web Client program or a browser.

HyperText Transport Protocol	HTTP	The protocol for moving Hypertext files across the Internet. Requires an HTTP client program on one end, and an HTTP server program on the other end. HTTP is the most important protocol used in the World Wide Web.
Import		Taking a document that already exists in electronic form, converting the file format to TIFF, if needed, and storing it in the Department's EDMS.
Incident		A violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing that a specific incident is about to occur. (Source: Section 282.0041, Florida Statutes)
Indexing		The process of recording the specific structured data that describes the electronic records in EDMS.
Infonet		The Department's internal information network also referred to as the Intranet.
Information Asset	IA	A definable piece of information, stored in any manner, which is recognized as valuable to the Department. The information that comprises an information asset may be little more than a vendor name and vendor address file, or it may be a complete report such as the monthly "Production Report".
Information Asset Author		The Information Asset Author is a person or persons who created and/or perform maintenance on an Information Asset linked to in the EIP system.
Information Asset Owner		The Information Asset Owner is a person or persons with authority over and responsible for the content of an Information Asset linked to in the EIP system.
Information Owner		Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. See Information Steward. (Source: Rule 74-2.001, F.A.C.)
Information Resource Coordinator		The role assigned to an individual responsible for maintaining access controls for a particular information resource or environment.
Information Resource Management		The planning, budgeting, acquiring, developing, organizing, directing, training, and control associated with government information resources. The term encompasses information and related resources, as well as the controls associated with their acquisition, development, dissemination, and use.

Information Resource Management Council	IRMC	Comprises the following three (3) voting members: the Assistant Secretary for Finance and Administration (Chair), the Assistant Secretary for Engineering and Operations, and the Assistant Secretary for Intermodal Systems Development. The IRMC reviews major information resource management projects, applications, or initiatives prior to the expenditure of funds or the commencement of work. The Chief Information Officer (CIO) serves as a non-voting member of the Council.
Information Resource Request	IRR	Used to submit computer and technology related product requests to the Office of Information Systems for review and approval.
Information Resources/Information Technology Resources	ITR	Data, automated applications, and information technology resources as defined in subparagraph 71A-1.002(43), F.A.C. and Sections 282.0041(14) and 282.101, F.S. Information resources include any transmission, emission, and reception of signs, signals, writings, images, and sounds of intelligence of any nature by wire, radio, optical, or other electromagnetic systems and includes all facilities and equipment owned, leased, or used by all agencies and political subdivisions of state government, and a full-service information-processing facility offering hardware, software, operations, integration, networking, consulting services, and other standalone environments, such as those used by ITS.
Information Security		The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Source: Rule 74-2.001, F.A.C.)
Information Security Manager	ISM	The person appointed pursuant to Section 282.318(4)(a), F.S. (Source: Rule 74-2.001, F.A.C.) The Department's internal and external point of contact for all information security matters.
Information Security Program		A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, to assure adequate security for agency information and information technology resources. (Source: Rule 71A-1.002, F.A.C.) The purpose of the Program is to support the Department's mission and establish controls to ensure adequate security for all information processed, transmitted or stored in Department automated information systems, e.g., information technology security plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

Information Technology	IT	Equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. (Source: Section 282.0041, Florida Statutes)
Information Technology Disaster Recovery Plan	ITDRP	Information technology resources and procedures to ensure the availability of critical resources needed to support the agency mission in the event of a disaster and to return to normal operations within an accepted timeframe. The ITDRP takes into account availability requirements, recovery time frames, recovery procedures, back-up/mirroring details, systematic and regular testing and training. (Source: Rule 71A-1.002, F.A.C.)
Information Technology Infrastructure		Network devices, server hardware, and host operating systems, database management systems, utilities, and other assets required to deliver or support IT services. (Source: Rule 71A-1.002, F.A.C.)
Information Technology Policy		A definite course or method of action selected from among one or more alternatives that guide and determine present and future decisions. (Source: Section 282.0041, Florida Statutes)
Information Technology Resources		A broad term that describes a set of technology related assets. While in some cases the term includes items such as people and maintenance, as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data Section 282.0041(13), F.S. (Source: Rule 74-2.001, F.A.C.)
Information Technology Services		Any information technology related services acquired through the Department’s procurement processes.
Information Technology Worker		An agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see User; Worker; Workforce). (Source: Rule 74-2.001, F.A.C.)
Integrity		The principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.
Intellectual Property		Data, including programs. (Source: Section 815.03, Florida Statutes)
Interactive Session		A work session where there is an exchange of communication between a user and a computer. (Source: Rule 71A-1.002, F.A.C.)

Internet		A worldwide system of interconnected governmental, educational, commercial, and private networks linked by common network technologies.
Internet Subscriber Account	ISA	
Intranet		A computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization. This term is used in contrast to extranet, a network between organizations. Sometimes, the term refers only to the organization's internal website but may be a more extensive part of the organization's information technology infrastructure, and may be composed of multiple local area networks. (Compare to **Extranet**.)
IT Manual		Department-wide policies and procedures relating to information technology.
IT Standards		A specific set of requirements to regulate how a system or organization provides services; required practices, controls, components, or configurations established by a recognized authority.
Jail Broken or Rooted		Also referred to as 'rooted'. To gain privileged control over or access to the operating system of a smart phone, tablet, or information technology resource, usually in order to run modified or unauthorized software or to alter system files or settings typically inconsistent with the manufacturer's intent.
Joint Application Development	JAD	Collaborative workshop approach.
Joint Application Requirements	JAR	Collaborative workshop approach.
Least Privilege		The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (Source: Rule 74-2.001, F.A.C.)
Link		Also known as a Hyperlink or a Web link. A word, phrase, picture, or icon in a document on which a user may click to move to another part of the document or to a different webpage or document. If the link is text-based, it is usually blue and underlined and changes colors once accessed.
Local Agency Program Information	LAPIT	
Local Area Network	LAN	

Mainframe		A deprecated term that relates to a server that runs the z/OS operating system, now known as the zEnterprise Server. Since mainframe is a commonly understood term here at the Department, references to mainframe are still used in this document.
Maintenance		Programming changes needed to keep an application performing according to its specifications, generally without changing its functionality. Maintenance includes defect repair, hardware or software upgrades, data conversion (mapping data or programs from one format to another), user support and preventive maintenance activities (changes to prevent future defects or failures) on a routine, mandated, or emergency basis.
Maintenance Release		The implementation of a set of fixes or enhancements, received as Requests for Service, for an existing application system maintained by the Application Services Bureau. These requests are completed as a unit and placed into production within a stated period of time. The work required and the resources available determine the length of the release. Most releases do not exceed six (6) months. A maintenance release contract is developed to identify the Request(s) for Service that will be accomplished during the release.
Major Information Resource Project, Application, or Initiative		Information resource management projects, applications, or initiatives that (1) involve more than one district; or (2) have an outcome that impacts multiple districts; (3) exceed $ 500,000 in total cost over a 1-year period (12 months); or (4) IT purchases in excess of $250.
Malware		A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. (Source: Rule 74-2.001, F.A.C.)
Management Controls		The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. (Source: Rule 74-2.001, F.A.C.)
Management Steering Committee	MSC	The MSC provides functional management oversight for the portal. This committee is responsible for providing project direction, strategy and planning for the portal.
Media		Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (Source: Rule 74-2.001, F.A.C.)

Method and Practice		Internal policies and procedures relating to the Office of Information Technology.
Mobile Computing Device		A portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones). (Source: Rule 71A-1.002, F.A.C.)
Mobile Device		A general term describing both mobile computing and mobile storage devices. (Source: Rule 71A-1.002, F.A.C.)
Mobile Device Management	MDM	An enterprise level solution which is used to secure and deploy over-the-air applications, data and configuration settings for all types of mobile computer devices for the agency.
Mobile Storage Device		Portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices. (Source: Rule 71A-1.002, F.A.C.)
Move Request		A feature of PANAPT which serves as the on-line request in PANAPT (options on the mainframe ISPF panels) to specify the software component(s) to be migrated and the anticipated date of migration.
National Institute of Standards and Technology	NIST	A non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration. (Source: Rule 71A-1.002, F.A.C.)
Need to Know		A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (Source: Rule 74-2.001, F.A.C.)
Nesting (Nested) Group		Microsoft Windows supports the concept of nesting groups, or adding groups to other groups. Nesting groups can help reduce the number of permissions that need to be individually assigned to users or groups. (Source: MSDN Library)
Network		Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (Source: Rule 74-2.001, F.A.C.)
Network Perimeter		The boundary of an agency's information technology infrastructure. (Source: Rule 71A-1.002, F.A.C.)
Network, Computer		A set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities. (Source: Section 815.03, Florida Statutes)

Next Gen		A standing quality improvement team within the Office of Information Technology (OIT) responsible for assignments relating to issues and activities that significantly impact one or more OIT unit. Next Gen advises and provides recommendations to OIT management on IT issues. (Formerly **Technical Advisory Group**.)
Non-Standard		No existing standard.
Office Manager		The Select Exempt Service (SES) or Senior Management Service (SMS) level manager for an office referenced by this procedure. If an office does not have an SES level manager, the Office Manager is the SMS level manager.
Office of Information Systems	OIS (FDOT)	No longer active. See **Office of Information Technology**.
Office of Information Technology	OIT	The division-level office within the Department of Transportation that is responsible for providing DOT with a functional statewide information processing and communications network. Responsibilities include providing controls for information resources in the area of procurement, security and finance; providing support for the Department's integrated office automation systems; and managing all computer-based administration and managerial data processing information. (Formerly **Office of Information Systems**.)
OIT Application Coordinator	OIT AC	An Office of Information Technology employee designated as the primary contact for coordinating development and maintenance services for specific applications. OIT ACs are designated for all applications for which the Office of Information Technology is the custodian and are responsible for (1) assessing the work effort involved for maintenance requests and the resulting impact to other work efforts; (2) coordinating with the functional application coordinator to establish priority levels for requests; (3) effectively applying resources to the requests; and (4) overseeing the work performed. (See **Office of Information Technology**.)
OIT Application Services Contract Manager		The OIT Application Services Contract Manager is the individual that is in the position of Contract Manager. The Contract Manager is in charge of ensuring all invoices are tracked, recorded, and reported correctly to the OIT Business Office for processing and payment.
OIT Application Services Contract Manager – Delegate		The delegate is an individual that the OIT Application Services Contract Manager has designated to perform the tracking, recording and reporting duties for the invoice process. The delegate cannot provide final management sign off on the invoice.
OIT Management Team		The CIO and the managers of Application Services, IT Services, Information Security, and Integration Services. (See **Office of Information Technology**.)

OIT Policy and Procedure Program Coordinator		A position (person) identified in OIT to ensure OIT policies, procedures, and directives are kept up-to-date. This position is also responsible for performing quality assurance reviews (QAR) on these policies, procedures, and directives within OIT offices. (See **Office of Information Technology**.)
OIT Policy and Procedures Review Library		The OIT Policy and Procedure review library is a centralized website that is set up for all OIT staff to view documents within the library, however, only members of the OIT Procedures Review team may post entries in the library. (See **Office of Information Technology**.)
OIT Procedure Review Team		The OIT management team, the OIT Policy and Procedure Program Coordinator, delegates, a representative from the Office of Inspector General, and the Information Security Manager (ISM).
OIT Quality Assurance Program Coordinator		This position is responsible for performing quality assurance reviews (QAR) on policies, procedures, and directives within OIT offices. (See **Office of Information Technology**.)
Operational Controls		Security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems). (Source: Rule 74-2.001, F.A.C.)
Operational Information Security Plan		The agency plan governing the information security program. In addition to detailing the activities, timelines and deliverables for the security objectives that, subject to current resources, the agency will implement during the current fiscal year, the plan includes a progress report for the prior fiscal year, related costs that cannot be funded from current resources, and a summary of agency compensating controls. (Source: Rule 71A-1.002, F.A.C.)
Outside Agency		A governmental agency that contracts to use the Department computer facilities. This may include use by local government agencies engaged in transportation related projects or other state agencies.
Outside Agency Representative		Someone with authority to legally bind the outside agency by signature.
Owner (of an Information Resource)		The manager of the business unit ultimately responsible for an information technology resource. (Source: Rule 71A-1.002, F.A.C.)

PANsophic Automated Production Turnover	PANAPT	Also known as CA/PANAPT. Automated production turnover software residing on the mainframe used to (1) automate the retrieval of mainframe computer application components from production libraries, (2) store the retrieved component to non-production libraries for development or maintenance tasks, (3) migrate mainframe computer application components to production libraries, and (4) compile, link/bind the application component(s).
Password		A protected string of characters which serves as authentication of a person's identity ("personal password"), which may be used to grant or deny access to private or shared data ("access password").
Patch Management		The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. (Source: Rule 74-2.001, F.A.C.)
Peer to Peer		A communications model that allows the direct sharing of files (audio, video, data, and software) among computers. (Source: Rule 71A-1.002, F.A.C.)
Performance Metrics		The measures of an organization's activities and performance. (Source: Section 282.0041, Florida Statutes)
Personal Firewall		A utility on a computer that monitors network activity and blocks communications that are unauthorized. (Source: Rule 74-2.001, F.A.C.)
Personal Information		An individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements: (a) Social Security Number. (b) Driver's license number or Florida Identification Card number. (c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Note: as provided in Sections 501.171(1)(g)1 and 817.5681, F.S., the term personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. (Source: Rule 74-2.001, F.A.C.)
Personally-Owned Device		A device in which is not owned, leased, or maintained by the agency but has been approved to access Florida Department of Transportation (FDOT) technology resources.
Personnel, Department		All SES, SMS, Career Service and OPS employees, consultants, contractors, volunteers, trainees and other persons whose job function in the performance of work for the Department is under the direct control of the department.
Platform		The software/hardware configuration on which an application resides (i.e. mainframe, LAN/WAN/SAN, web-based, databases, or any combinations of these).

Plug-in (for browsers)		Downloadable files that are executed to enhance the capability of a browser. Examples include Adobe Acrobat Reader and QuickTime View.
Portal		An internal website that provides proprietary, enterprise-wide information as well as access to selected public websites and vertical-market websites (suppliers, vendors, etc.). It may include a search engine for internal documents as well as the ability to customize the portal page for different user groups and individuals. It is the internal equivalent of the general-purpose portal on the Web.
Primary Internet Server		The Intranet server containing the Department's Intranet home page and navigation pages for the Department's Intranet. This server provides a locator function for all Department Intranet environments. This server is the responsibility of OIT.
Privately-Owned Device		A device not purchased with agency funds; a device owned by a person or other non-agency entity and not configured, maintained, or tracked by the agency. (Source: Rule 71A-1.002, F.A.C.)
Procurement Documents		Requisitions, contracts, purchasing card, or other documents used to acquire information technology resources.
Production Control Section		The section responsible for (among other duties) the function of migrating computer application components to the specific production libraries. This section is also responsible for operation of the PANAPT software on the mainframe.
Production Infrastructure		Network devices, server hardware, and host operating systems that comprise an agency's operational or real-time environment. (Source: Rule 71A-1.002, F.A.C.)
Production Jobs		Any set of established and pre-defined instructions which executes programs or modules against production data or files on a routine or scheduled basis to support the functionality of a system.
Production Libraries		The secured computer libraries where computer application components reside for the purpose of performing the Department's business functions.
Production Migration		The managed (planned, organized, directed and controlled) process for moving approved computer application components into production libraries and environments.
Production Staging Area		A secured library, directory, file or web site where computer application components reside prior to being migrated to the production library(ies).

Program, Computer		A set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions. (Source: Section 815.03, Florida Statutes) This includes, but is not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications, and computer networking programs.
Project		An endeavor that has a defined start and end point; is undertaken to create or modify a unique product, service, or result; and has specific objectives that, when attained, signify completion. (Source: Section 282.0041, Florida Statutes)
Project Coordinator		A Department employee responsible for coordinating the project, application, or initiative being submitted for review and approval by the Information Resource Management Council.
Project Development Methodology	PDM	The documented process by which the Department develops new applications and maintain existing ones. The PDM establishes the standards for how information systems are developed, identifies the required documentation for those information systems, and identifies the roles and responsibilities of the personnel involved in the application development process.
Project Estimating Group	PEG	A team of OIT members that are charged with reviewing business cases and providing a third-party level of effort estimate based on all known facts, historical data, and expert judgment. The PEG convenes on an as-needed or as-requested basis to produce project estimates.
Project Manager		A Department employee who ensures that the terms and conditions of contracts are properly executed.
Project Oversight		An independent review and analysis of an information technology project that provides information on the project's scope, completion timeframes, and budget and that identifies and quantifies issues or risks affecting the successful and timely completion of the project. (Source: Section 282.0041, Florida Statutes)
Project Team Estimate	PTE	An estimate that is developed by members of the actual project team, and that is based on knowledge of application requirements. PTEs should be done each time there is a change request, or new iteration in order to achieve the most accurate estimate possible.
Property		Anything of value as defined in s. 812.012 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in machine-readable or human-readable form, and any other tangible or intangible item of value. (Source: Section 815.03, Florida Statutes)
Protocol		Formal rules that computers must follow to communicate.

Public Information Office	PIO	Provides communications support for the Department through a Central Public Information Office in Tallahassee and eight district public information offices. Directs the public information efforts of consultants on major projects. Communicates Department policy to the public and department employees. Develops long range public information goals and objectives.
Public Records		All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency.
Public Records Act		Refers to Chapter 119, F.S. (Source: Rule 71A-1.002, F.A.C.)
Quality Assurance Review	QAR	The QAR's process is to collect and analyze collected data from each District, ensure the Districts are in compliance with policies and procedures and offer any corrective action recommendations, if any. A final compliance report will be issued 120 days after the QAR closes.
Quality Assurance Tasks	QA	The activity of providing fact-based evidence that quality products, services, and information are being delivered.
Quality Control Tasks	QC	The activities of implementing, monitoring and continuously improving processes to ensure delivery of quality products, services, and information.
Regression Test		Testing used to confirm, any or all of the following: defects have been fixed; new defects have not been introduced; and that features that were proven correctly functional are intact.
Reimage		The process of removing and deleting any previously stored data and software on a computer and reinstalling, in its place, pre-configured operating system and software.
Relational Database Management System	RDBMS	A database management sysytem based on the relational model.
Remote Access		Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). (Source: Rule 74-2.001, F.A.C.)
Resource Access Control Facility	RACF	This is the primary management system for security authorization within the Department and contains user-IDs for all authorized users of the Department's information technology resources.
Return Merchandise or Material Authorization	RMA	A transaction whereby the recipient of a defective product arranges its return to the supplier to have the product repaired or replaced or in order to receive a refund or credit for another product from the same retailer or corporation.

Review		A formal or official examination of system records and activities that may be a separate agency prerogative or a part of a security audit. (Source: Rule 71A-1.002, F.A.C.)
Risk		The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (Source: Rule 74-2.001, F.A.C.)
Risk Analysis		The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (Used interchangeably with risk assessment.) (Source: Rule 74-2.001, F.A.C.)
Risk Assessment		The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. (Source: Section 282.0041, Florida Statutes)
Risk Management		The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; (3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and (4) documenting the overall risk management program. (Source: Rule 74-2.001, F.A.C.)
Sanitizing		Using a utility that provides a minimum of three passes of overwriting all addressable locations with a character, its complement, then a random character and verifying. DOD 5220.22-M requirements accomplish this. This includes erasing data and/or reformatting magnetic tape media.
Script		A script is a list of commands that can be executed without user interaction. A script language is a simple programming language with which you can write scripts. Examples of scripting languages (for the Web) are: Java, JavaScript, JScript; VBScript.
Secure Socket Layers	SSL	Security technology for establishing an encrypted link between a web server and a browser.
Secure Sockets Layer Virtual Private Network	SSLVPN	A communications network tunneled through another communications network with an encrypted link between a web server and a browser.
Security Administrator, Computer		The role assigned to individuals that are specialized in securing and supporting various areas of the FDOT infrastructure. These administrators are approved by the ISM and serve as statewide technical resources for Computer Security Coordinators and the FDOT Enterprise Security team.

Security Controls		The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed to protect the confidentiality, integrity, and availability of information technology resources. (Source: Rule 74-2.001, F.A.C.)
Security Coordinator, Computer		The role assigned to individuals that are responsible for monitoring and implementing security controls and ensuring compliance with procedures for applications or information technology environments. A Traditional Select Exempt Service (SES) or Senior Management Service (SMS) manager selects computer security coordinators. There are two different types of computer security coordinators: Information Resource Coordinators and Functional Application Coordinators.
Security Incident		A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. See Incident (Source: Rule 74-2.001, F.A.C.)
Security Incident, Computer		Any confirmed real or suspected adverse event in relation to the security of information, information technology resources, or both.
Security Review		An examination of system records and activities to determine the adequacy of system controls, ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any indicated changes in any of the foregoing. (Source: Rule 71A-1.002, F.A.C.)
Security Team, FDOT Enterprise		The group within ETSS that is responsible for operational security issues.
Security User ID Resource Facility	SURF	
Security, Computer		Measures that implement and assure security in a computer system, particularly those that assure access control; usually understood to include functions, features and technical Characteristics of computer hardware and software, especially operating systems.
Select Exempt Service (SES) Manager Procedure		This procedure pertains to the traditional SES manager, not Service First SES personnel, who is defined as SES in a Level 3 Manager, Pay Band 21, or Level 4 – Manager, Pay Band 22, position; or a position with a DMS comparable class of Regional Toll Manager-DOT in Level 2 – Manager, Pay Band 21.
Selected Exempt Service	SES	
Senior Management Service	SMS	
Senior Management Service	SMS	

Separation of Duties		An internal control concept of having more than one person required to complete a critical process. This is an internal control intended to prevent fraud, abuse, and errors. (Source: Rule 74-2.001, F.A.C.)
Server		A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running. A single server machine could have several different server software packages running on it, thus providing many different services to clients on the network.
Service Account		The ISM has defined this type of account as being 'non-interactive' used by a system or application (e.g. service, scheduled task, batch process etc.) Interactive logon for these accounts shall be executed only after it has been communicated via our official change notification/management system.". These accounts will only be logged onto "locally" when the service, for which they are requested and authorized, is being set up initially or being maintained. If emergency work is deemed necessary by the local District IT Service Manager (DITSM) or IT Cost Center Manager, local logon with service account may be performed prior to an approved change request, but not in lieu of one. Service accounts shall have alerts built in FDOT Log Management software that will send notice to the CSIRT team (email distribution list). The CSIRT team will review and establish if the account was used without an approved change control and issue an incident if no local DITSM approval existed for an emergency usage of the service account. (Source: Rule 74-2.001, F.A.C.)
Service Desk		A point of contact for information technology service needs. Service Desks provide customer-focused interfaces, assisting information technology resource users throughout the Department, enabling the efficient use of services, helping restore normal services as soon as possible, and being proactive in advising users of potential service interruptions.
Service Level		The key performance indicators (KPI) of an organization or service which must be regularly performed, monitored, and achieved. (Source: Section 282.0041, Florida Statutes)
Service Level Agreement	SLA	A written contract between the state data center and a customer entity which specifies the scope of services provided, service level, the duration of the agreement, the responsible parties, and service costs. A service-level agreement is not a rule pursuant to chapter 120. (Source: Section 282.0041, Florida Statutes)

Services, Data Processing		All services that include, but are not limited to, feasibility studies, systems design, software development, or time-sharing services.
Session		The time during which two devices maintain a connection and are usually engaged in transferring data or information. (Source: Rule 71A-1.002, F.A.C.)
Session Initiated Protocol	SIP	
Site Owner		SMS level manager or traditional SES manager, as defined in the preceding definition, who is responsible for maintaining a Department website.
Smart Card		A credit card-sized card with embedded integrated circuits that can store, process, and communicate information. (also known as integrated circuit card). (Source: Rule 74-2.001, F.A.C.)
Sniffing		Capturing network data. (Source: Rule 71A-1.002, F.A.C.)
Software, Common Standard		An operating system, a word processing package, or a spreadsheet package that meets Department standards.
Software, Computer		A set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions. (Source: Section 815.03, Florida Statutes) This includes, but is not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications, and computer networking programs.
Solid State Drive	SSD	Device that uses integrated circuit assemblies as memory to store data persistently.
Source Code		The computer code for the software printed or displayed in human readable form.
Special Trust or Position of Trust		Positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment, pursuant to Section 110.1127, F.S. (Source: Rule 71A-1.002, F.A.C.)
Sponsor, SMS/SES Office Manager		The Senior Management Service or Select Exempt Service office manager supporting or sponsoring the project, application, or initiative being submitted for review and approval by the Information Resource Management Council.

Staff Augment		Contracted personnel serving specific business objectives within the workplace, who supplement a Cost Center's workforce and operate under the direct supervision of an FDOT project manager or supervisor. For a contracted personnel to be considered staff augment, the following conditions must apply: the contracted personnel must be provided workspace within an FDOT facility in order to perform work assignments, the contracted personnel must be assigned an FDOT e-mail address, the contracted personnel must support internal staff from within an FDOT facility, and the contracted personnel must work 'face-to-face' with users or staff on projects. (See also: **Consultant**)
Staff Augmentation		Staff Augmentation is defined as an outsourcing strategy which is used to staff a project and respond to business objectives. The technique consists of evaluating the existing staff and then determining which additional skills are required.
Stakeholder		A person, group, organization, or state agency involved in or affected by a course of action. (Source: Section 282.0041, Florida Statutes)
Standard Configuration		Documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems. (Source: Rule 71A-1.002, F.A.C.)
Standard Hardware		Agency-approved hardware. (Source: Rule 71A-1.002, F.A.C.)
Standard Software		Agency-approved software. (Source: Rule 71A-1.002, F.A.C.)
Standards		A published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard. (Source: Rule 74-2.001, F.A.C.)
Standards and Quality Management	SQM	The Standards and Quality Management Team supports the mission of OIT, Application Services and the Department, by implementing strategy, standards, analysis, and quality practices to assure the quality of all OIT products and services.
Standards and Technical Work Group	STWG	The governing body for new and existing technology standards, as well as exceptions to standards.
State Agency		Any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. As used in part I of this chapter, except as otherwise specifically provided, the term does not include the Department of Legal Affairs, the Department of Agriculture and Consumer Services, or the Department of Financial Services. (Source: Section 282.0041, Florida Statutes)

State Chief Information Security Officer		The State of Florida executive responsible for the state government information security posture and direction. This position is appointed by the state Chief Information Officer and oversees the state Office of Information Security. (Source: Rule 71A-1.002, F.A.C.)
State Data Center	SDC	The State Data Center is dedicated to providing safe, secure housing for data processing equipment and applications.
State Office of Information Security	OIS (State)	The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their risks so effective security controls can be implemented. The OIS is part of the Agency for Enterprise Information Technology, pursuant to Section 282.318(3), F.S. (Source: Rule 71A-1.002, F.A.C.)
Strategic Enterprise Architecture and Infrastructure Team	SEAIT	Strategic Enterprise Architecture and Infrastructure Team (SEAIT) will advance and support enterprise infrastructure and application architecture to assist the department in successfully building and supporting applications on an Enterprise level. Provide services and support of Database Platforms, Business Intelligence, Windows Servers, EDMS, GIS and the FEL libraries.
Strategic Information Security Plan		The agency three-year plan that defines security goals, intermediate objectives, and projected agency costs for the strategic issues of information security policy, risk management, security training, security incident response, and survivability. (Source: Rule 71A-1.002, F.A.C.)
SUNCOM Network		The state enterprise telecommunications system that provides all methods of electronic or optical telecommunications beyond a single building or contiguous building complex and used by entities authorized as network users under this part. (Source: Section 282.0041, Florida Statutes)
Support Personnel, Computer		Support personnel responsible in the areas of network support, client application support, and desktop support.
Surplus		Electronic media and devices that are no longer used by the Department and shall not be owned by the Florida Department of Transportation. These items are typically donated or RMA returns to other entities or organizations outside the Florida Department of Transportation or are destroyed to prevent further use.
Survivability		The capability of an organization to maintain or quickly recover critical business functions after a disaster or adverse event, minimize the effect of an event, reduce financial loss, and expedite the return to normalcy. (Source: Rule 71A-1.002, F.A.C.)

System		Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (Source: Rule 74-2.001, F.A.C.)
System Administrator		A person who manages the technical aspects of a system. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (Source: Rule 74-2.001, F.A.C.)
System Hardening		The process of securing a system. Hardening typically includes ensuring proper configurations based on intended function, removing non-essential programs and utilities, disabling certain accounts, and installing patches. (Source: Rule 71A-1.002, F.A.C.)
System Security Plan	SSP	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. (Source: Rule 74-2.001, F.A.C.)
System Test		Tests designed to validate the application against the user requirements.
System Test Libraries	SYSTEST	The libraries where computer application components reside for the purpose of testing, prior to being migrated to the production library(ies) or environments.
Tailgating		The passage of unauthorized personnel, either forced or accidental, behind that of an authorized user.
Technical Advisory Group	TAG	No longer active. See **Next Gen**.
Technical Controls		Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (Source: Rule 74-2.001, F.A.C.)
Technical Review		A review conducted to ensure that a proposed information asset meets all applicable technical standards, and procedures. This review will evaluate the information asset and its data, to ensure that it is protected, available, reliable, and consistent.

Technology Refresh		A technology refresh occurs when the technology supporting an application (database, platform, or software) changes so significantly that upgrading the application to take advantage of the advances in technology is necessary. An application that is a candidate for a technology refresh generally meets one or more of the following criteria: (a) the current technology will no longer be supported by the vendor; (b) significant gains in computing speed, ease-of-use, or enhanced interfaces with other systems can be made; or (c) the users will benefit from the additional functionality provided by the upgraded software or hardware without the need to make significant programming modifications to the application system in order to do so.
Technology Request System	TRS	Allows users to request a variety of services from the Office of Information Systems. The TRS System includes Information Resource Requests (IRR), Automated Access Request Forms and the Software Distribution Notification System.
Technology Services & Support	TSS	No longer active. As part of the TSSO, TSS provided end user support statewide and was geographically located within the Department's seven districts (D1-D7), State Materials Office (SMO), and Central Office (CO). TSS was regionally managed by a Technology Services and Support Manager, or TSSM.
Technology Services and Support Manager	TSSM	No longer active. (Formerly **District Information System Manager**.)
Technology Services and Support Office	TSSO	No longer active. Now a combination of IT Services and Integration Services bureaus, which provide the Department's districts and Central Office with a functional computer network infrastructure, support for the Department's wide area network (WAN) and technical support for voice communications statewide. The Department's direction is to achieve its business objectives through the implementation of CPR-compliant standards. As such, these bureaus strive to standardize its best practices and operate in a consistent, predictable, and repeatable environment statewide. They conduct the daily operations of the Department's seven district data centers and the State Materials Office. They provide these offices and the Central Office with administration and management of network resources, computer security, information technology purchasing assistance, support for computer hardware and peripherals and support for standard software applications. Support in each District and Central Office is managed by an OIS Manager. (Formerly **District Information Systems Office**.)
Telecommunications		The science and technology of communication at a distance, including electronic systems used in the transmission or reception of information. (Source: Section 282.0041, Florida Statutes)

Test Infrastructure		A technical environment that mirrors part or all of the production environment and is used for final testing of a technology or an application prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure. (Source: Rule 71A-1.002, F.A.C.)
Test Plan Strategy		A means of communicating testing matters such as organization of testing, strategic choices concerning organization, and execution.
Threat		Any circumstance or event that has the potential to adversely impact a state agency's operations or assets through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service. (Source: Section 282.0041, Florida Statutes)
Track		The documented assignment of an asset to a user and/or location. (Source: Rule 71A-1.002, F.A.C.)
Trade Secret		The whole or any portion or phase of any formula, pattern, device, combination of devices, or compilation of information which is for use, or is used, in the operation of a business and which provides the business an advantage, or an opportunity to obtain an advantage, over those who do not know or use it.
Traditional Select Exempt Service (SES) Manager Procedure		This procedure pertains to the SES manager in a Level 3 – Manager, Pay Band 21, or Level 4 – Manager, Pay Band 22, position; or a position with a DMS comparable class of Regional Toll Manager-DOT in Level 2 – Manager, Pay Band 21. This does not include Service First SES personnel.
Transfer		Changes in ownership of electronic media and devices from one Cost Center to another Cost Center. This can be within or across Districts. Ownership of transferred items always remains within the Florida Department of Transportation's chain of custody.
Transitory Messages		A message containing limited administrative value, and that does not set or change policy, establish guidelines or procedures, or certify a transaction.
Transmission Control Protocol/Internet Protocol	TCP/IP	A set of rules or protocols that was developed for internetworking over both the network layer and transport layers. Computers must use TCP/IP to transmit data and exchange messages via the Internet.
T-Shirt Size		The estimated size of a project according to the following scale:Small (0-250 hours)Medium (251-5,000 hours)Large (5,001-10,000 hours)Extra-Large (>10,000 hours)
Unit Testing		The testing of a single application component or module in order to test the detailed logic and accuracy of performance. Unit testing is generally performed by the programmer of the module. Unit testing does not test how well the individual module works with other modules, that type of testing is done during system testing.

User		Any authorized entity that uses information technology resources (see **Worker**; **Workforce**; **Information Technology Worker**). (Source: Rule 71A-1.002, F.A.C.) This includes State employees, contractors, vendors, third parties, trainees, and volunteers in a part-time or full-time capacity.
User Identification Code	User-ID	A data item associated with a specific individual, who represents the identity of that individual within a computer system and may be known by other individuals. User-ID is used interchangeable with other terms such as 'user account' and could also be referencing other accounts, e.g. generic and/or service account.
User, Computer		Any authorized entity who uses information technology resources (interchangeable with User). (Source: Rule 74-2.001, F.A.C.)
User, New		A system entity, usually a human individual, who does not possess authorization to access the Department's information technology resources and who is seeking authorization to access the Department's information technology resources.
Variance		A calculated value that illustrates how far positive or negative a projection has deviated when measured against documented estimates within a project plan. (Source: Section 282.0041, Florida Statutes)
Vendor		A company that is external from the FDOT that provides experienced individuals to work in a strategic role on a project and respond to the business objectives the Department.
Virtual Private Network	VPN	A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks. (Source: Rule 74-2.001, F.A.C.)
Voice Over Internet Protocol	VOIP	
Warning Banner		A message displayed prior to or upon connection to a resource informing the user that activities may be monitored or access is restricted. (Source: Rule 71A-1.002, F.A.C.)
Web Application		Computer software designed to help the user perform specific tasks via a Web browser.
Web Author		An individual responsible for the creation or maintenance of content for a Web page, Web site, or Web application.
Web Page		The presentation of content on the Internet and/or Intranet.
Webmaster		A team within Application Services that is responsible for supporting FDOT Web authors by providing assistance, training, troubleshooting and compliance reviews.
Website		A set of related Web pages served from a single Web domain.
Wide Area Network	WAN	

Wireless Devices		Mobile information technology resources that contain a wireless network interface card and can wirelessly transmit data or voice communications over a network. (See also: **Mobile Device**.)
Work Plan, Application Services Bureau		The document that identifies all Application Services projects and the resources allocated for a given fiscal year. Projects in the Work Plan are identified as (1) maintenance, (2) enhancements or (3) application development and are rated as (a) urgent, (b) mandated or (c) routine.
Worker		A member of the workforce. A worker may or may not use IT resources. This includes employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency. (see User; Workforce; Information Technology Worker). (Source: Rule 74-2.001, F.A.C.)
Workforce		Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker; Information Technology Worker). (Source: Rule 74-2.001, F.A.C.)
World Wide Web	WWW	The environment of hypertext servers which have been established to allow text, graphics, sound files, etc., to be mixed together and used for world wide public access.