CHAPTER 5

ELECTRONIC SECURITY FOR PUBLIC RECORDS EXEMPTIONS

PURPOSE:

To establish a process for providing security for the Department's electronic records that are exempt public records, provide guidance in determining which records are exempt public records, and to establish standards for the protection of those records. Any questions regarding the confidential and exempt status of a record should be referred to the Department's Office of the General Counsel prior to releasing or authorizing the release of such information.

AUTHORITY:

Section 20.23(3)(a) and 334.048(3), Florida Statutes

SCOPE:

This procedure applies to all records processed through information systems within the Department.

REFERENCES:

Chapter 119, Florida Statutes
Section 282.318, Florida Statutes
Section 337.168(1) and 337.14(1), Florida Statutes
Section 768.28 (16)(b) Florida Statutes
Section 812.081, Florida Statutes
Section 815.04, Florida Statutes

BACKGROUND:

Section 119.01, F.S., requires that all state, county, and municipal records, unless exempt, shall at all times be open for a personal inspection by any person. Furthermore, all agencies must provide reasonable public access to records electronically maintained and must ensure that confidential or exempt records are not disclosed except as otherwise permitted by law.

Section 282.318, F.S., requires the designation of the Department's Information Security Manager (ISM), whose responsibility shall be to administer the security program of the Department for data and information technology resources.

5.1 EXEMPT DOCUMENTS

5.1.1 All records of the Florida Department of Transportation are public records subject to disclosure, except those specifically made confidential or exempt by law. Public records which are confidential or exempt are subject to special security considerations. The following are examples of some of the more common exemptions. A more complete list may be found in the ***Government in the Sunshine Manual*** prepared by the Office of the Attorney General and printed by the First Amendment Foundation.

5.1.2 A document or electronic file revealing the official cost estimate by the Department of a project is confidential and exempt from the provisions of ***Section 119.07(1), F.S.***, until the contract for the project has been executed or until the project is no longer under active consideration. ***(Section 337.168(1), F.S.)***

5.1.3 A document revealing the identity of persons who have requested or obtained bid packages, plans or specifications pertaining to any project to be let by the Department is confidential and exempt from the provisions of ***Section 119.07(1), F.S.***, for the period which begins two business days prior to the deadline for obtaining bid packages, plans, or specifications and ends with the letting of the bid. ***(Section 337.168(2), F.S.)*** Prior to the two business days, these documents remain public record.

5.1.4 Any financial statement which an agency requires a prospective bidder to submit in order to prequalify for bidding or for responding to is exempt from the provisions of ***Section 119.07(1), F.S.***, (***Section 119.071(1)(c), F.S.***).

5.1.5 The Bid Analysis and Monitoring System (BAMS) of the Department is confidential and exempt from the provisions of ***Section 119.07(1), F.S.*** This exemption applies to all system documentation, input, computer processes and programs, electronic data files, and output, but does not apply to the actual source documents unless otherwise exempted under other provisions of law. ***(Section 337.168(3), F.S.)*.**

5.1.6 Any person desiring to bid for the performance of any construction contract in excess of $250,000 must first be certified by the Department as qualified. Information detailing the contractor's equipment, past records, experience, financial resources, and personnel is confidential and exempt from the provisions of ***Section 119.07(1), F.S. (Section 337.14(1), F.S.).***

5.1.7 Sealed bids, proposals, or replies received by an agency pursuant to invitations to bid or requests for proposals are exempt from the provisions of ***Section 119.071(1), F.S.***, until such time as the agency provides notice of a decision or intended decision or within 30 days after bid, proposal opening, or final replies whichever is earlier. **(*Section 119.071(1)(b), F.S.*).**

5.1.8 Public records prepared by, or at the express direction of, an agency attorney which reflect mental impressions, conclusions, litigation strategy or legal theory of the attorney or agency and which were prepared exclusively for civil or criminal litigation or adversarial administrative proceedings or in anticipation of imminent civil or criminal litigation or adversarial administrative proceedings are exempt from the provisions of ***Section 119.07(1), F.S.***, until the conclusion of such litigation or proceedings **(*Section 119.071(1)(d), F.S.*).**

5.1.9 Aspects of agency security planning responsibilities pursuant to ***Section 282.318, F.S.***, the ***Security of Data and Information Technology***, shall be confidential and exempt from the provisions of ***Section 119.07(1), F.S.***, except that such information shall be available to the Auditor General, the Cybercrime Office of the Department of Law Enforcement, the Agency for State Technology, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General. This includes:

(A) Risk Analysis information to determine security threats to the data, information and information technology resources. This includes both the information gathered and the final report **(*Section 282.318(4)(d), F.S.*).**

(B) Results of periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency **(*Section 282.318(4)(g), F.S.*).**

(C) Written internal policies and procedures for the security of data and information technology resources which, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources. These documents shall be distributed only to those persons responsible for information security in a given area, and not to the user community in general, except such information shall be available to the Auditor General in performing his post auditing duties **(*Section 282.318(4)(j), F.S.*).**

(D) Written internal policies and procedures for reporting security incidents **(*Section 282.318(4)(e), F.S.*).**

(E) Records that identify detection, investigation or response practices for suspected or confirmed security incidents**(*Section 282.318(4)(j), F.S.*).**

5.1.10 Claim files of the Division of Risk Management, Department of Insurance, some of which are maintained in the Department's Office of the General Counsel, are confidential and exempt from the provisions of ***Section 119.07(1),*** until termination of all litigation and settlement of all claims arising out of the same incident, pursuant to ***Section 768.28 (16)(b)F.S.***

5.1.11 Certain Personnel records, including social security numbers, medical records, and the personal information of protected employees and their families, are confidential and exempt from the provisions of ***Section 119.07(1), F.S.*** (***Section 119.071 (4)(5), F.S.*****).**

5.1.12 Complaints and other records relating to a complaint or charge of employment discrimination are exempt from the provisions of ***Section 119.07(1) F.S***. until a finding is made regarding probable cause, the investigation of the complaint or charge becomes inactive, or the complaint or charge is made part of the official record at any hearing or proceeding. ***(Section 119.071(2)(g)(1) F.S.).***

5.1.13 Plans, blueprints, schematic drawings, and diagrams, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility or other structure owned or operated by an agency, are exempt from the provisions of ***119.07(1) F.S. (Section 119.071(3)(b) F.S.)*** These records may be provided to a licensed architect, engineer, or planner performing work on or related to the structure, or to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities, or upon showing of good cause in Court. ***(Section 119.071(3)(b) F.S.)***

5.1.14 Records that relate directly to the physical security of the facility or security system plans or portions thereof held by an agency are confidential and exempt from the provisions of ***Section 119.07(1) F.S. (Section 119.071 (3)(a) F.S.).*** The confidential records may be released to the property owner or leaseholder; or another state or federal agency relative to the prevention, detection, investigation, or prosecution of an attempt or act of terrorism. ***(Section 119.071 (3)(a) F.S.).***

5.1.15 When the Department seeks to acquire real property by purchase or through the exercise of eminent domain, appraisals and other reports relating to values, offers and counteroffers are exempt from the provisions of ***Section 119.07(1)*** until execution of a valid option contract or written offer to sell that has been conditionally accepted by the agency, at which time the exemption expires. The Department may also exempt title information, including names and addresses of property owners whose property is

subject to acquisition to purchase through the exercise of the power of eminent domain, to the same extent as appraisals, other reports relating to value, offers and counteroffers. ***(Section 119.0711 F.S.).***

5.1.16 Bank account numbers and debit, charge, and credit card numbers held by an agency are exempt from ***Section 119.071(1) F.S.*** and ***Section 119.071(5)(b) F.S.***

5.1.17 Any information obtained by the Department as a result of research and development projects and revealing a method or process, production, or manufacture which is a trade secret as defined in ***Section 688.002(4), F.S.*** is confidential and exempt from the provisions of ***Section 119.07(1) F.S.*** and ***Section 334.049(4) F.S.***

5.1.18 Certain information and investigatory records of the Inspector General related to an active investigation in accordance with ***Section 20.055(7) F.S.***, are confidential and exempt from the provisions of ***Sections 119.071 and 119.011 F.S. and Section 112.3188 F.S.*** Records prepared and collected by the Office of Inspector General, while carrying out its statutory investigative duties and responsibilities in accordance with ***Section 20.055(7), F.S.***

(A) For a complaint of misconduct filed against an agency employee until the investigation ceases to be active, ***Section 119.071(2)(k)1, F.S.***

(B) Where the Office of Inspector General (OIG) has reasonable grounds to believe there has been a violation of criminal law, ***Section 119.011(3)(d), F.S.***

(C) To assist a law enforcement agency in the conduct of an active criminal investigation or prosecution, ***Section 119.071(2)(c)1, F.S.***

(D) Where the OIG is engaged in a joint investigation or assisting a law enforcement agency or prosecutor, ***Section 119.011(3)(d), F.S.***

5.1.19 Crash reports that reveal the personal information concerning the parties involved in the crash and that are held by any agency that regularly receives or prepares information from or concerning the parties to motor vehicle crashes are confidential and exempt from the provisions of ***Section 119.07(1) F.S.*** for a period of 60 days after the date the report is filed. ***(Section 316.066(2)(a) F.S.).***

5.1.20 Personal identifying information provided to, acquired by, or in the possession of the Department, a county or expressway authority for the purpose of using a credit card, charge card, or check for the prepayment of electronic toll facilities charges to the Department, a county, or an expressway authority is exempt from ***Section 119.07(1) F.S***. ***(Section 338.155(6) F.S.)*.**

5.1.21 Trade Secret Information, as defined in ***Section 812.081, F.S.***, relating to data, programs, or supporting documentation that is trade secret, pursuant to ***Section 812.081, F.S.***, which resides or exists internal or external to a computer, computer system, computer network, or electronic device which is held by an agency, is confidential and exempt from the ***Public Records Law (Section 815.04(3), F.S., Section 815.045, F.S. and Section 119, F.S.).***

5.1.22 Data processing software obtained by an agency under a licensing agreement that prohibits its disclosure and which software is a trade secret, as defined in ***Section 812.081, F.S.***, and agency-produced data processing software that is sensitive are exempt from the ***Public Records Law***; however, an agency-head is not prohibited from sharing or exchanging such software with another public agency. ***(Section 119(1)(f), F.S.)***

5.1.3 A document that reveals the identity of a person who has requested or obtained a bid package, plan, or specifications pertaining to any project to be let by the department before the two working days prior to the deadline for obtaining bid packages, plans, or specifications remain a public record subject to ***Section 119.07(1) F.S.***

5.2 Those electronic records which are exempt or confidential by law from the provisions of the ***Public Records Law*** shall not be released to any person without legal review by the Office of the General Counsel. Any questions regarding the confidential or exempt status of a document should be referred to the Department's Office of the General Counsel prior to releasing or authorizing the release of such information.

5.3 Owners of confidential or exempt electronic records described above are responsible for the security of that information. If the records are created, edited, stored, read, deleted, or transmitted electronically, the owner is responsible for:

(A) Documenting the access of persons permitted access and to what degree within the Department’s Automated Access Request Forms (AARF) system;

(B) Updating access within the Automated Access Request Forms (AARF) system whenever the access list changes or conditions pertinent to the records change;

(C) Providing written assurance, at least annually, to the ISM (or their designee) that the security of the records has been reviewed and that the access list is accurate.

(D) Ensuring that those persons permitted access to confidential electronic data are held responsible for the security of any extract or report that they derived from that data, in any format whatsoever.

TRAINING:

None required.

FORMS:

None required.