THE FULL TEXT OF THE PROPOSED RULES IS:

64B19-18.0025 Qualifications to Practice Juvenile Sexual Offender Therapy.

Effective December 31, 2005, a psychologist ~~October 1, 2000 an individual~~, prior to practicing ~~holding oneself out as a~~ juvenile sexual offender therapy ~~therapist~~, must be a Florida licensed psychologist, except as otherwise provided within Section 490.012, F.S. ~~Chapter 98-158, Laws of Florida~~. The psychologist ~~individual~~ shall have education, training, and experience that demonstrates competency and interest in this area of practice. The training of a psychologist practicing juvenile sexual offender therapy ~~therapist~~ must include: 1) coursework and/or training ~~at least nine hours of coursework~~ in child behavior and development, ~~and in~~ child psychopathology, and child assessment and treatment; and 2) thirty (30) hours of training in juvenile sex offender assessment and treatment ~~integrated with juvenile assessment, diagnosis, and treatment~~.

Specific Authority 490.004(4), 490.012(8), 490.0145 FS. Law Implemented 490.012(8), 490.0145 FS. History–New 2-21-99, Amended _____.

64B19-18.006 Prohibition Against Treating Psychologists Performing Forensic Evaluations of Minors for the Purpose of Addressing Custody, Residence or Visitation.

Specific Authority 490.004(4) FS. Law Implemented 490.009(2)(s) FS. History–New 6-14-94, Formerly 61F13-20.006, Amended 2-8-96, Formerly 59AA-18.006, Repealed _____.

(Substantial rewording of Rule 64B19-18.007 follows. See Florida Administrative Code for present text.)

64B19-18.007 Requirements for Forensic Psychological Evaluations of Minors for the Purpose of Addressing Custody, Residence or Visitation Disputes.

(1) For the purposes of this rule the following definitions apply:

(a) "Parent" means parent or legal guardian identified by the court order.

(b) "Child(ren)" means those identified by the court order.

(2) The minimum standard of performance in court-ordered child custody evaluation and family law proceedings includes, but is not limited to, the following:

(a) The psychologist shall adhere to the APA Guidelines for Child Custody Evaluations in Divorce Proceedings, and the specialty guidelines for Forensic Psychologists and all pertinent Florida law.

(b) The psychologist who has accepted an appointment as an evaluator shall not serve as guardian ad litem, mediator, therapist or parenting coordinator regarding the children in the instant case. The psychologist who has had a prior role as guardian ad litem, mediator, therapist or parenting coordinator shall not accept an appointment as an evaluator for the children in the instant case.

(c) The psychologist shall inform the parents or legal guardian in writing and obtain their signature verifying notification of the limits of confidentiality.

(d) The psychologist shall submit the evaluation report pursuant to court order or provide prior notification to the court, if the report will not be provided by the due date.

(e) The evaluation report shall include all of the following. The failure to include any of the following shall be documented.

1. Evaluations of both parents, or legal guardian including observations, test results, and impressions.

2. Evaluations of the children identified in the court order including observations and where appropriate, test results and impressions.

3. Description of interactions between each parent or legal guardian and each child identified in the court order.

4. Collateral sources of information as needed.

5. Request medical records as needed.

(3) It is a conflict of interest for a psychologist who has treated a minor or any of the adults involved in a custody or visitation action to perform a forensic evaluation for the purpose of recommending with which adult the minor should reside, which adult should have custody, or what visitation should be allowed. Consequently, a psychologist who treats a minor or any of the adults involved in a custody or visitation action may not also perform a forensic evaluation for custody, residence or visitation of the minor. A psychologist may provide a court, or a mental health professional performing a forensic evaluation, with factual information about the minor derived from treatment, but shall not state an opinion about custody, residence or visitation disputes.

Specific Authority 490.004(4) FS. Law Implemented 490.009(2)(s) FS. History–New 6-14-94, Formerly 61F13-20.007, Amended 1-7-96, Formerly 59AA-18.007, Amended _____.

NAME OF PERSON ORIGINATING PROPOSED RULE: Board of Psychology

NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE: Board of Psychology

DATE PROPOSED RULE APPROVED BY AGENCY HEAD: April 15, 2004

DATE NOTICE OF PROPOSED RULE DEVELOPMENT PUBLISHED IN FAW: 64B19-18.0025 (Feb. 24, 2004); 64B19-18.006 (Nov. 21, 2003); 64B19-18.007 (Dec. 27, 2002)

Section III
Notices of Changes, Corrections and Withdrawals

DEPARTMENT OF EDUCATION

State Board of Education

RULE NO.:	RULE TITLE:
6A-10.044	Residency for Tuition Purposes

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 30, No. 16, April 16, 2004, Florida Administrative Weekly has been withdrawn.

BOARD OF TRUSTEES OF THE INTERNAL IMPROVEMENT TRUST FUND

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Board of Trustees of the Internal Improvement Trust Fund are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."

REGIONAL PLANNING COUNCILS

South Florida Regional Planning Council

RULE NO.:	RULE TITLE:
29J-2.009	Strategic Regional Policy Plan for South Florida

NOTICE OF HEARING CHANGE

A Notice of Proposed Rule for the above referenced Rule was published in the May 14, 2004 edition of the FAW. The location of the hearing has been changed.

A HEARING WILL BE HELD AT THE TIME, DATE AND PLACE SHOWN BELOW:

TIME AND DATE: 10:30 a.m., June 7, 2004

PLACE: Hawk's Cay Resort, 61 Hawk's Cay Blvd., Duck Key, Florida 33050

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Robert Daniels, South Florida Regional Planning Council, 3440 Hollywood Boulevard, Suite 140, Hollywood, FL 33021, (954)985-4416

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NO.:	RULE TITLE:
60A-1.001	Definitions

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 30, No. 17, April 23, 2004, Florida Administrative Weekly, has been withdrawn.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NO.:	RULE TITLE:
60A-1.003	Forms

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 30, No. 17, April 23, 2004, Florida Administrative Weekly, has been withdrawn.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NOS.:	RULE TITLES:
60A-1.009	Emergency Purchases of Commodities or Contractual Services
60A-1.010	Single Source Purchases of Commodities or Contractual Services
60A-1.011	Identical Responses Received
60A-1.025	State Purchasing Agreements
60A-1.047	Alternate Contract Sources of Commodities and Services

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rules in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 10, March 5, 2004 issue of the Florida Administrative Weekly:

PROPOSED RULE 60A-1.009, F.A.C., WAS CHANGED TO READ AS FOLLOWS:

60A-1.009 Emergency Purchases of Commodities or Contractual Services.

(1) Filing Notice with the Department. Section 287.057(5)(a), F.S. defines the term "emergency purchase," and details the requirements an agency must follow in making an emergency purchase of commodities or services. In order to comply with the reporting requirement therein, agencies must file with the Department Form PUR 7800 (03/04), "Notice of Emergency Purchase," which is hereby incorporated by reference, within thirty (30) days after date of issuance of the emergency purchase order or contract. This form is available on the internet at http://dms.myflorida.com/purchasing.

(2) through (4) No change.

Specific Authority 287.042(12) FS. Law Implemented 287.001, 287.057(5)(a) FS. History–New 2-6-68, Revised 5-20-71, Amended 7-31-75, 10-1-78, 8-6-81, 11-12-84, 12-17-85, Formerly 13A-1.09, Amended 11-3-88, 1-18-90, 4-10-91, Formerly 13A-1.009, Amended 1-9-95, 7-6-98, 1-2-00, _____.

PROPOSED RULE 60A-1.010, F.A.C., WERE CHANGED TO READ AS FOLLOWS:

60A-1.010 Single Source Purchases of Commodities or contractual Services.

Single source purchases are purchases of commodities or contractual services available only from a single source. Pursuant to Section 287.057(5)(c), F.S., such purchases are excepted from the competitive solicitation process.

(1) Posting of Description of Intended single Source Purchase. If an agency believes that a commodity or contractual service is available only from a single source and the total cost is in excess of the threshold for Category Two, the agency shall electronically post Form PUR 7776 (02/04), "Description of Intended Single Source Purchase," which is

hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing. This notice shall be posted for at least seven (7) business days.

(2) No change.

(3) Final Determination if Total Cost does not exceed Category Four. After making the written determination required by paragraph 2 above, if the total cost of the single source purchase does not exceed Category Four the agency shall provide notice of its decision to enter into a single source purchase by utilizing Form PUR 7778 (02/04), "Notice of Intended Decision to Enter Into a Single Source contract," which is hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing. This notice must be electronically posted in accordance with Section 120.57(3), F.S.

(4) No change.

(a) Certification Filed with Department. The certification and request for approval must be submitted to the Department using Form PUR 777 (02/04), "Single Source Certification and Request for Approval," which is hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing. The submission must be made via electronic mail and must be addressed to singlesource@dms.state.fl.us.

(b) Department Review of Certification. The Department shall review all requests properly submitted and shall approve or disapprove all requests within 21 days of receipt. Failure by the Department to respond to a request within 21 days of receiving a request or receiving additional requested information shall constitute approval of the request. ~~If the Department requests additional information from the agency in order to make its determination, the 21 day period begins anew.~~ The Department shall approve all requests submitted if the agency has provided all required documentation in accordance with Section 287.057 (5)(c), F.S. and this rule. The requesting agency retains authority and responsibility to determine whether or not a single source is justified. Agencies are encouraged to review Section 838.22(2), F.S. regarding circumvention of competitive bidding processes.

(c) No change.

(5) through (7) No change.

Specific Authority 287.042(12) FS. Law Implemented 287.001, 287.057(5) FS. History–New 2-6-68, Revised 5-20-71, Amended 8-6-81, 2-28-85, 12-17-85, Formerly 13A-1.10, Amended 11-3-88, 1-18-90, 4-10-91, Formerly 13A-1.010, Amended 1-9-95, 1-1-96, 9-23-96, 7-6-98, 1-2-00, _____.

PROPOSED RULE 60A-1.011, F.A.C., WAS CHANGED TO READ AS FOLLOWS:

60A-1.011 Identical Responses Received.

(1) Criteria. When evaluating vendor responses to solicitation, if the agency is confronted with identical pricing or scoring ~~(as applicable)~~ from multiple vendors, the agency shall determine the order of award using the following criteria, in the order of preference listed below (from highest priority to lowest priority):

(a) through (2) No change.

Specific Authority 287.042(12) F.S. Law Implemented 287.051(1),(12), 287.082, 287.084, 287.087, 287.092 FS. History–New 2-6-68, Revised 5-20-71, Amended 7-31-75, 10-1-78, 8-6-81, 2-13-83, 10-13-83, 3-1-84, Formerly 13A-1.11, Amended 11-3-88, 4-10-91, Formerly 13A-1.011, Amended _____.

PROPOSED RULE 60A-1.025, F.A.C., WERE CHANGED TO READ AS FOLLOWS:

60A-1.025 State Purchasing Agreements.

(1) Requesting a State Purchasing Agreement. State Purchasing Agreements are driven by eligible users' requirements, and eligible users shall ~~may~~ request that the Department establish such agreements by submitting to the Department PUR 7721 (02/04), "Request for State Purchasing Agreement," which is hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing. The commodity or service the eligible user wishes to acquire must be valued at less than Category Two in order to comply with the competitive solicitation requirement of Section 287.057, F.S.

(2) Establishing a State Purchasing Agreement. After receiving PUR 7721 for an eligible user, the Department will attempt to establish a State Purchasing Agreement with a supplier offering the best value for the requested commodity or service. The supplier must agree to the terms contained in PUR 7722 (02/04), "State Purchasing Agreement," which is hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing.

Specific Authority 287.042(12) FS. Law Implemented 287.042(2)(a) FS. History–New _____.

PROPOSED RULE 60A-1.047, F.A.C., WERE CHANGED TO READ AS FOLLOWS:

60A-1.047 Alternate Contract Sources of Commodities and Services.

(1) Requests for alternate contract source approval. Agencies may request permission from the Department to purchase commodities or services from term contracts or requirements contracts competitively established by other governmental entities. Agencies must submit Form PUR 7102 (03/04), "Agency Request for Review of Alternate Contract Source," which is hereby incorporated by reference, in order to request permission. This form is available on the internet at http://dms.myflorida.com/purchasing. The contract must contain specific language or other legal authority authorizing third parties to make purchases from the contract with the vendor's consent.

(2) No change.

(3) Department identification of alternate contract sources. The Department shall ~~may~~ independently identify term contract or requirements contracts awarded by other governmental entities, and approve such alternate contract sources for use by agencies. The Department shall only approve those alternate contract sources that are cost-effective and in the best interest of the State."

(4) Alternate contract sources available online. The Department shall maintain on its website a list of all current alternate contract sources and the agencies authorized to use such contracts. The Department's website is http://dms.myflorida.com.

(5) No change.

Specific Authroity 287.042(12) FS. Law Implemented 287.042(16) FS. History–Formerly 60A-1.008(3)(b), Amended _____.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Richard L. Brown, Division of State Purchasing, Department of Management Services, 4050 Esplanade Way, Tallahassee, FL 32399, (850)488-3049

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NOS.:	RULE TITLES:
60A-1.012	Purchasing Categories and Adjustments Thereto
60A-1.016	Contract and Purchase Order Requirements
60A-1.021	Electronic Posting of Decisions and Intended Decisions
60A-1.042	Request for Information
60A-1.063	Present Value Methodology

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rules in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 14, April 2, 2004 issue of the Florida Administrative Weekly:

60A-1.012 Purchasing Categories and Adjustments Thereto.

~~(1) Purchasing Categories. The following threshold categories are established:~~

~~(a) Category One: $15,000.~~

~~(b) Category Two: $25,000.~~

~~(c) Category Three: $50,000.~~

~~(d) Category Four: $150,000.~~

~~(e) Category Five: $250,000.~~

(1)~~(2)~~ Adjustments to Purchasing Categories. State Purchasing will ~~may~~ adjust the dollar amount for the purchasing categories based on the April publication of the United State Department of Commerce Survey of current Business Table 7.11B, using the price index for state and local government. The amounts for the threshold categories will be adjusted as follows:

(a) The rate of adjustment applicable to the threshold amounts is the percent increase or decrease in the chain-type price index from the base year value for 1992, which is 97.9, through the year previous to the year of annual adjustment as shown in the United States Department of Commerce Survey of Current Business as referenced above.

(b) This rate of adjustment is applied to the base threshold amounts to calculate the threshold amount for the year of adjustment.

The following formula illustrates this method: Threshold for Year of Adjustment = Base Threshold × [Price Index in April Publication for the Year Prior to the Year of Adjustment divided by 97.9]

(2)~~(3)~~ Timing and Application of Categories. Notwithstanding the pint in time in which payment is made for the commodities or services, for the purpose of applying the threshold categories to a purchase, the earliest of the following dates shall govern:

(a) The date on which the solicitation is issued.

(b) The date the purchase order is issued.

(c) The date on which the contract is entered into.

Specific Authority 287.042(12), 287.017(2) FS. Law Implemented 287.017 FS. History–Formerly 60A-1.001(10), Amended _____.

60A-1.016 Contract and Purchase Order Requirements.

(1)(a) Prior to making a purchase, an agency shall ~~should~~ review current surplus property certifications ~~to utilize commodities listed therein to the maximum extent practicable~~.

(b) All purchases shall be in writing or through the State's Purchasing Card Program.

(2)(a) A written agreement in excess of the threshold amount of Category Two shall be signed by the agency head and the vendor prior to the rendering of the contractual services ~~and/~~or the delivery of the commodity, expect in the case of a valid emergency as certified by the agency head. If the agency chooses to procure commodities or contractual services by purchase order in lieu of a written agreement, the purchase order shall be signed by the authorized purchasing or contracting personnel. When there is no emergency and the agency fails to have the written agreement signed as required, the agency head, no later than 30 days after the vendor begins rendering the service ~~and/~~or delivering the commodity, shall certify the conditions and circumstances as well as action taken to prevent reoccurrence, to State Purchasing using the "Notice of Non-Compliance," Form PUR 1010 (03/04), which is hereby incorporated by reference. This form is available on the internet at http://dms.myflorida.com/purchasing. Pursuant to Section 287.058(2), F.S., the agency shall also send a copy of this form to the chief Financial Officer with the voucher authorizing payment.

(b) Any contract which binds the state or its executive agencies for purchases for a period continuing beyond the fiscal year shall include the following statement: "The State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Legislature."

~~(c) Any contract between an agency and a private contract vendor shall contain the language provided in Sections 946.515(6) and 413.036(3), F.S., if at the time the contract is entered into, any product or service which is the subject of, or required to be carried out, the contract has been certified by the Department of Management Services as a correctional work program item or is on the procurement list of the qualified nonprofit agency for the blind or for the other severely handicapped.~~

(c)~~(d)~~ All contracts that limit the liability of a contractor shall be consistent with Section 672.719, F.S.

(3) Purchase Order Requirements. To the extent that these requirements are not superceded by an electronic procurement system, the chief procurement officer of each agency is responsible for:

(a) Securing all unused purchase orders in a safe place and restricting access to these documents.

(b) Maintaining a file and accounting system for all consecutive purchase orders issued or voided.

(c) Maintaining a record of persons authorized to issue and sign each type of purchase order.

(d) Monitoring and reviewing processes for the use of purchase orders and field purchase orders.

(e) Ensuring ~~The agency is also responsible for ensuring~~ that all purchase orders contain the solicitation number ~~(if applicable)~~, statements regarding the quantity, description, and price of goods or services ordered; applicable terms as to payment, discount, date of performance, and transportation; and liquidated damages~~, if appropriate~~.

Specific Authority 287.032, 287.042 FS. Law Implemented 287.017, 287.042, 287.057, 287.058, 287.133 FS. History–New 8-6-81, Amended 11-4-82, 2-13-83, 5-26-83, 10-13-83, 5-10-84, 11-12-84, 12-17-85, Formerly 13A-1.16, Amended 6-5-86, 2-9-87, 11-3-88, 1-18-90, 4-10-91, Formerly 13A-1.016, Amended 4-24-94, 1-9-95, 1-1-96, 3-24-96, 7-6-98, 1-2-00, _____.

60A-1.021 Electronic Posting of Decisions and Intended Decisions.

~~(1)~~ All agency decisions or intended decisions (as defined in Rule 28-110.002, F.A.C.) shall be electronically posted on the myflorida.com website. All competitive solicitations issued by agencies pursuant to Sections 287.051(1)-(3), F.S., shall be advertised by electronic posting for no less than 10 calendar days prior to the date for receipt of responses, unless the agency determines in writing that a shorter period of time is necessary to avoid harming the interests of the state. ~~All competitive solicitations issued by agencies pursuant to Sections 287.057(1) (3), F.S. shall be advertised by electronic posting for no less than 10 calendar days prior to the date for receipt of responses. If the agency head or his or her designee determines that an unusual problem exists and the 10 day period would be detrimental to the interest of the agency, the agency head or the designee shall document the contract file with the conditions and circumstances requiring waiver of advertising for less than 10 calendar days.~~

Specific Authority 287.042(12) FS. Law Implemented 287.042(3)(b)(2) FS. History–Formerly 60A-1.002(4), Amended _____.

60A-1.042 Request for Information.

(1) An agency may request information by issuing a written ~~electronically posting a~~ Request for Information. Agencies may use Requests for Information in circumstances including, but not limited to, determining whether or not to competitively procure a commodity or contractual services, determining what solicitation process to use for a particular need, or researching general, special, and/or technical specifications for a solicitation.

(2) A vendor's answer to a Request for Information is not an offer and the agency may not use the vendor's submission to justify a contract with that vendor without otherwise complying with Chapter 287, F.S. and Rule 60A-1, F.A.C.

(3) Vendors submitting answers to an agency's Request for Information are not prohibited from responding to any related subsequent solicitation.

Specific Authority 287.042(12) FS. Law Implemented 287.012(21), 287.042(3)(g) FS. History–New _____.

60A-1.063 Present Value Methodology.

All competitive solicitations that include provisions for ~~contracts which require payment for more than one (1) year and include~~ unequal payment streams or unequal time periods shall include a condition stating that the evaluation will use present value methodology. The solicitation shall state the present value discount rate, which will be used in the computations and evaluation.

To determine that appropriate discount rate, agencies shall use the rates identified in Release H.15, Select Interest Rates (Weekly), available online at http://www.federalreserve.gov/releases/h15/. Agencies shall ~~should~~ use the most recent release and the appropriate U.S. treasury rate for the last published month at the time of issuance of the competitive solicitation.

Specific Authority 287.0572(2) FS. Law Implemented 287.0572(1) FS. History–Formerly 60A-1.002(7)(d), Amended _____.

THE PERSON TO BE CONTACTED REGARDING THE PROPOSED RULE IS: Richard L. Brown, Division of State Purchasing, Department of Management Services, 4050 Esplanade Way, Tallahassee, FL 32399, (850)488-3049

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NO.:	RULE TITLE:
60A-1.073	Alteration of Responses Not Permitted

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 30, No. 14, April 2, 2004, Florida Administrative Weekly, has been withdrawn.

DEPARTMENT OF MANAGEMENT SERVICES

Division of Purchasing

RULE NO.:	RULE TITLE:
60A-1.074	Request to Withdraw Solicitation

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 30, No. 14, April 2, 2004, Florida Administrative Weekly, has been withdrawn.

DEPARTMENT OF MANAGEMENT SERVICES

Agency for Workforce Innovation

RULE NOS.:	RULE TITLES:
60BB-2.0255	Annual Filing
60BB-2.037	Public Use Forms

NOTICE OF CORRECTION

The Department of Management Services, Agency for Workforce Innovation, announces the following correction to the proposed rules as published in the Florida Administrative Weekly on February 27, 2004 (Vol. 30, No. 9, pp. 875-876).

The "NAME OF SUPERVISOR OR PERSON WHO APPROVED THE PROPOSED RULE" should read: Tom Clendenning, Deputy Director for Unemployment Compensation, Agency for Workforce Innovation, 107 E. Madison Street, MSC 229, Tallahassee, Florida 32399-4135; and, Bruce Hoffmann, General Counsel, Department of Revenue, P. O. Box 6668, Tallahassee, Florida 32314-6668, (850)488-0712.

DEPARTMENT OF MANAGEMENT SERVICES

State Technology Office

RULE NOS.:	RULE TITLES:
60DD-2.001	Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management
60DD-2.004	Logical and Data Access Controls
60DD-2.006	Network Security
60DD-2.007	Backup and Disaster Recovery
60DD-2.008	Personnel Security and Security Awareness
60DD-2.009	Systems Acquisition, Auditing, and Reporting
60DD-2.010	Standards Adopted

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rules in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 11, March 12, 2004, issue of the Florida Administrative Weekly:

60DD-2.001 Purpose; Definitions; Policy; Applicability; Agency Security Programs; Roles and Responsibilities; Risk Management.

(1) Purpose.

(a) Rules 60DD-2.001-60DD-2.010, Florida Administrative Code, shall be known as the Florida Information Resource Security Policies and Standards.

(b) The purpose of the Florida Information Resource Security Policies and Standards is to:

1. Promulgate state policies regarding the security of data and information technology resources. Policies are broad principles underlying the state's information resource security program.

2. Define minimum-security standards for the protection of state information resources. Standards are required administrative procedures or management controls, utilizing current, open, non-proprietary or non-vendor specific technologies.

(c) Nothing in this rule chapter shall be construed to impair the public's access rights under Chapter 119, Florida Statutes, and Article I, Section 24 of the Florida Constitution.

(2) Definitions.

(a) The following terms are defined:

1.~~(a)~~ Access – To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

2.~~(b)~~ Access control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

3.~~(c)~~ Access password – A password used to authorize access to data and distributed to all those who are authorized similar access.

4.~~(d)~~ Access Point – A station that transmits and receives data

5.~~(e)~~ Advanced Encryption Standard or "AES"– A Federal Information Processing Standard (FIPS 197) developed by NIST to succeed DES. Intended to specify an unclassified, publicly disclosed, symmetric encryption algorithm, available royalty-free worldwide, to protect electronic data.

6.~~(f)~~ Agency – Those entities described in Section 216.011(1)(qq), Florida Statutes.

7.~~(g)~~ Asymmetric encryption – A modern branch of cryptography (sometimes called "public-key cryptography") in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

8.~~(h)~~ Attack – An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to violate the security of a system.

9.~~(i)~~ Audit – See: Security Audit.

10.~~(j)~~ Authentication – The process that verifies the claimed identify or access eligibility of a station, originator, or individual as established by an identification process.

11.~~(k)~~ Authorization – A positive determination by the information resource/data owner or delegated custodian that a specific individual may access that information resource, or validation that a positively identified user has the need and the resource/data owner's permission to access the resource.

12.~~(l)~~ Availability – The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise causes a denial of service of system resources.

13.~~(m)~~ Back door – A hardware or software mechanism that (a) provides access to a system and its resources by other than the usual procedure, (b) was deliberately left in place by the system's designers or maintainers, and (c) usually is not publicly known.

14.~~(n)~~ Business continuity plan – See: Disaster-Preparedness Plan.

15.~~(o)~~ Best Practice – a technique or methodology that, through experience and research, has proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success.

16.~~(p)~~ Block cipher – An encryption algorithm that breaks plaintext into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of cipher-text.

17.~~(q)~~ Central Computer Room – A facility dedicated to housing significant computing resources, such as mainframe computers and libraries; commonly referred to as a data center.

18.~~(r)~~ Client – A system entity that requests and uses the service provided by another system entity called a "server".

19.~~(s)~~ Comprehensive Risk analysis – A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first.

20.~~(t)~~ Computer Security – 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.

21.~~(u)~~ Confidential information – Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Florida Public Records Act.

22.~~(v)~~ Confidentiality – The state that exists when confidential information is held in confidence and available only to a limited set of authorized individuals pursuant to applicable law. Confidentiality is the security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. ~~Confidentiality covers data in storage, during processing, and in transit.~~

23.~~(w)~~ Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery in a system as part of a security program to ensure availability of critical system resources and facilitate continuity of operations in a crisis. See: Disaster-Preparedness Plan.

24.~~(x)~~ Continuity of Operations Plan (COOP) – See: Disaster-Preparedness Plan.

25.~~(y)~~ Control – Any action, device, policy, procedure, technique, or other measure that improves security.

26.~~(z)~~ Critical information resource – That resource determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have an unacceptable impact.

27.~~(aa)~~ Current – Most recent; not more than one year old.

28.~~(bb)~~ Custodian of an information resource – Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, communications, protection controls, access controls, and output distribution for the resource; a person responsible for implementing owner-defined controls and access to an information source. The custodian is normally a provider of services.

29.~~(cc)~~ Data – A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means.

30.~~(dd)~~ "Data Encryption Algorithm" or "DEA" – A symmetric block cipher, defined as part of the United States Government's Data Encryption Standard. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.

31.~~(ee)~~ "Data Encryption Standard" or "DES" – A United States Government standard (Federal Information Processing Standard 46-3) that specifies the data encryption algorithm and states policy for using the algorithm to protect data.

32.~~(ff)~~ Data integrity – The condition existing when the data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

33.~~(gg)~~ Data security – The protection of data from disclosure, alteration, destruction, or loss that either is accidental or is intentional but unauthorized;

34.~~(hh)~~ Data security administrator – The person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Manager, agency management may designate a number of data security administrators.

35.~~(ii)~~ Denial of service – The prevention of authorized access to a system resource or the delaying of system operations and functions.

36.~~(jj)~~ "Disaster-Preparedness Plan" or "Continuity of Operations Plan" – An effort within individual departments and agencies pursuant to Section 252.365, Florida Statutes, to ensure the continued performance of minimum essential functions during a wide range of potential emergencies. An operational and tested information technology continuity plan should be in line with the overall agency disaster-preparedness plan and its related requirements and take into account such items as criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fallback and resumption plans, risk management activities, assessment of single points of failure, and problem management. Provisions should be documented in the plan and reviewed to establish back-up and off-site rotation of non-critical application software and job execution language libraries, data files, and systems software to facilitate restoration following recovery of critical applications.

37.~~(kk)~~ Encryption – Cryptographic transformation of data (called "plaintext") into a form (called "cipher-text") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption", which is a transformation that restores encrypted data to its original state. Encryption and decryption involve a mathematical algorithm for transforming data. In addition to the data to be transformed, the algorithm has one or more inputs that are control parameters: (a) a key value that varies the transformation and, in some cases, (b) an initialization value that establishes the starting state of the algorithm.

38.~~(ll)~~ End user – A system entity, usually a human individual, that makes use of system resources, primarily for application purposes as opposed to system management purposes. This includes State employees, contractors, vendors, third parties and volunteers in a part-time or full-time capacity.

39.~~(mm)~~ Environment – The aggregate of physical, organizational, and cultural circumstances, objects, or conditions surrounding an information resource.

40.~~(nn)~~ Exposure – Vulnerability to loss resulting from accidental or intentional unauthorized acquisition, use, disclosure, modification, or destruction of information resources.

41.~~(oo)~~ FIPS PUB (NR.) – Federal Information Processing Standard Publication (Nr.), a federal standard issued by the National Institute of Science and Technology (formerly the National Bureau of Standards).

42.~~(pp)~~ Information Custodians – agency employees responsible for assisting Information Owners in classifying data and specifying and implementing the technical mechanisms required to enforce policy to a degree of certainty required, based on a comprehensive risk analysis that considers the probability of compromise and its potential operational impact.

43.~~(qq)~~ Information Owners or "owner of an information resource" – agency managers who are responsible for specifying the security properties associated with the information their organization possesses and are responsible for the integrity and accuracy of that information. This includes what categories of users are allowed to read and write various items and what the operational impact of violations of policy would be.

44.~~(rr)~~ Information resources – Data, automated applications, and information technology resources as defined in subparagraph 60DD-2.001(2)(a)47.~~(vv)~~, Florida Administrative Code and Sections 282.0041(7) & 282.101, Florida Statutes.

45.~~(ss)~~ Information Security Alert – A notice sent by state agencies pursuant to paragraph 60DD-2.006(6)(b), Florida Administrative Code, regarding potential information security abnormalities or threats.

46.~~(tt)~~ Information Security Manager (ISM) – The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318(2)(a)1., Florida Statutes, and the agency's internal and external point of contact for all information security matters.

47.~~(uu)~~ "Information technology," "information technology resources" "information resources" or "information technology system" 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, and consulting services.

48.~~(vv)~~ Information Technology Security Plan or Information Resource Security Plan – A written plan periodically reviewed that provides an overview of the security requirements of the information systems and describes the controls in place or planned for meeting those requirements. It covers critical data policies, backup, disaster recovery, and user policies. Its purpose is to protect the integrity, availability, and confidentiality of IT resources (i.e., data, information, applications, and systems) and to support the missions of the State of Florida. The Information Technology Security Plan

also encompasses policies, procedures and guidelines together with methodology employed for protection, e. g. firewalls, user authentication, data encryption, key management, digital certificates, intrusion detection systems (IDS), virus detection, and virtual private networks (VPN).

49. Information Technology Security Program or Information Resource Security Program – A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, whose purpose is to support the agency's mission and establish controls to assure adequate security for all information processed, transmitted or stored in agency automated information systems, e.g., Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

50.~~(ww)~~ Integrity – The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

51.~~(xx)~~ Networks or networking – Networks provide design, programming, development and operational support for local area networks ("LANs"), wide area networks ("WANs") and other networks. Networks support client/server applications, telephony support, high-speed or real-time audio and video support and may develop and/or utilize bridges, routers, gateways, and transport media.

52.~~(yy)~~ NIST – National Institute of Standards and Technology.

53.~~(zz)~~ Password – A protected word or string of characters which serves as authentication of a person's identity ("personal password"), or which may be used to grant or deny access to private or shared data ("access password").

54.~~(aaa)~~ Personal identifier or user identification code - A data item associated with a specific individual, that represents the identity of that individual and may be known by other individuals.

55.~~(bbb)~~ Personal password – A password that is known by only one person and is used to authenticate that person's identity.

56.~~(ccc)~~ Platform – The foundation technology of a computer system. The hardware and systems software that together provide support for an application program and the services they support.

57.~~(ddd)~~ Provider – Third party such as contractor, vendor, or private organization providing products, services or support.

58.~~(eee)~~ Public Records Act – Section 119.01, et seq., Florida Statutes.

59.~~(fff)~~ Remote Access – The ability to connect to a computer from a remote location and exchange information or remotely operate the system.

60.~~(ggg)~~ 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.

61.~~(hhh)~~ Risk – The likelihood or probability that a loss of information resources or breach of security will occur.

62.~~(iii~~ Risk analysis – See: Comprehensive Risk Analysis.

63.~~(jjj)~~ Risk assessment – See: Comprehensive Risk Analysis

64.~~(kkk)~~ Risk management – Decisions and subsequent actions designed to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

65.~~(lll)~~ Router Transport Service – the State-wide multi-protocol fully routed data communications service.

66.~~(mmm)~~ Security audit – an independent formal review and examination of system records and activities to (a) determine the adequacy of system controls, (b) ensure compliance with established security policy and operational procedures, (c) detect breaches in security, and (d) recommend any indicated changes in any of the foregoing.

67.~~(nnn)~~ SSID – A Service Set Identifier – A sequence of characters that uniquely names a wireless local area network.

68.~~(ooo)~~ Security controls – Hardware, software, programs, procedures, policies, and physical safeguards that are put in place to assure the availability, integrity and protection of information and the means of processing it.

69.~~(ppp)~~ Security incident or breach – An event which results in loss, unauthorized disclosure, unauthorized acquisition, unauthorized use, unauthorized modification, or unauthorized destruction of information resources whether accidental or deliberate.

70.~~(qqq)~~ Security officer – See Data Security Administrator.

71.~~(rrr)~~ Security Risk Analysis – The process of identifying and documenting vulnerabilities and applicable threats to information resources.

72.~~(sss)~~ Security Risk Management – See Risk Management.

73.~~(ttt)~~ Security Standard – A set of practices and rules that specify or regulate how a system or organization provides security services to protect critical system resources.

74.~~(uuu)~~ Security Vulnerability Assessment – 1) An examination of the ability of a system or application, including current security procedures and controls, to withstand assault. A vulnerability assessment may be used to: a) identify weaknesses that could be exploited; and b) predict the effectiveness of additional security measures in protecting information resources from attack; 2) Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

75.~~(vvv)~~ Sensitive Locations – Physical locations such as a data center, financial institution, network operations center or any location where critical, confidential or exempt information resources can be accessed, processed, stored, managed or maintained.

76.~~(www)~~ Sensitive software – Software exempt under Section 119.07(3)(o), Florida Statutes; those portions of data processing software, including the specifications and documentation, used to: collect, process, store and retrieve information which is exempt from the Public Records Act under Section 119.07, Florida Statutes; collect, process, store and retrieve financial management information of the agency, such as payroll and accounting records; or control and direct access authorizations and security measures for automated systems.

77.~~(xxx)~~ Server – A system entity that provides a service in response to requests from other system entities called "clients".

78.~~(yyy)~~ Session – The time during which two computers maintain a connection and are usually engaged in transferring data or information.

79.~~(zzz)~~ Site Survey – A report on the physical, architectural, geographical and electrical limitations of the site and their effect on a wireless solution.

80.~~(aaaa)~~ Special Trust or Position of Trust – A position in which an individual can view or alter confidential information, or is depended upon for continuity of information resource imperative to the operations of the agency and its mission.

81.~~(bbbb)~~ Standard – See: Security Standard.

82.~~(cccc)~~ Storage or Computer Storage – The holding of data in an electromagnetic form for access by a computer processor; the process of storing information in computer memory or on a magnetic tape or disk.

83.~~(dddd)~~ Symmetric cryptography – A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key, such as the originator and the recipient of the message, need to keep the key secret.

84.~~(eeee)~~ System control data – Data files such as programs, password files, security tables, authorization tables, etc., which, if not adequately protected, could permit unauthorized access to information resources.

85.~~(ffff)~~ Third Party – See Provider.

86.~~(gggg)~~ Triple Data Encryption Standard or "Triple DES" or "3DES" – A block cipher, based on DES, that transforms each 64-bit plaintext block by applying a data encryption algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

87.~~(hhhh)~~ Unauthorized disclosure – A circumstance or event whereby an entity gains access to data for which the entity is not authorized.

88.~~(iiii)~~ Universal Access Service – State sanctioned secure, single point of access to enterprise applications and information.

89.~~(jjjj)~~ User – See: End User.

90.~~(kkkk)~~ Virtual Private Network or "VPN" – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

91.~~(llll)~~ Vulnerability – A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security.

92.~~(mmmmm)~~ Wi_Fi or Wireless Fidelity – The Wi-Fi Alliance certification standard signifying interoperability among 802.11b products.

93.~~(nnnn)~~ Wireless – Wireless includes any data communication device (e.g., personal computers, cellular phones, PDAs, laptops, etc) that is connected to any network of the State of Florida. This includes any form of Wireless communications device capable of transmitting packet data.

(3) Policy. Information technology resources residing in the various agencies are

(a) Documented and distributed security policies that incorporate the following issues:strategic and vital assets held in trust and belonging to the people of Florida. It is the policy of the State of Florida that information system security ensure the confidentiality, integrity and availability of information. A loss of confidentiality is the unauthorized disclosure of information. A loss of integrity is the unauthorized modification or destruction of information. A loss of availability is the disruption of access to or use of information or an information system. Each agency shall develop, implement, and maintain an information technology security program ~~plan~~ to be reviewed by the State Technology Office as set forth in this rule. All documents regarding the development, implementation and maintenance of such programs shall be maintained by the agency's Information Security Manager (ISM). Each agency shall develop, implement, and maintain an information resource security program ~~and plan(s)~~ that produces the following end products:

(a) Documented and distributed security policies that incorporate the following issues:

1. State information resources are valuable assets of the State of Florida and its citizens and must be protected from unauthorized modification, destruction, disclosure, whether accidental or intentional, or use. The acquisition and protection of such assets is a management responsibility.

2. Access requirements for state information resources must be documented and strictly enforced.

3. Responsibilities and roles of Information Security Managers and data security administrators must be clearly defined.

4. Information that, by law, is confidential or exempt must be protected from unauthorized disclosure, replication, use, destruction, acquisition, or modification.

5. Information resources that are essential to critical state functions must be protected from unauthorized disclosure, replication, use, destruction, acquisition, or modification.

6. All information resource custodians, users, providers, and his/her management must be informed of their respective responsibilities for information resource protection and recovery. These responsibilities must be clearly defined and documented.

7. All information resource custodians, users, providers, and his/her management must be informed of the consequences of non-compliance with his/her security responsibilities. These consequences must be clearly stated in writing.

8. Risks to information resources must be managed. The expense of implementing security prevention and recovery measures must be appropriate to the value and criticality of the assets being protected, considering value to both the state and potential intruders. Procedures for recording and responding to security breaches should be developed and disseminated to appropriate information resource custodians, users, providers, and their management, pursuant to each agency's internal security procedures.

9. The integrity of data, its source, its destination, and processes applied to it must be assured. Data must change only in authorized, predictable, auditable, and acceptable ways.

10. Information resource custodians, users, providers and their management must be made aware of their responsibilities in disaster-preparedness plans required to continue critical governmental services, to insure that information resources are available.

11. Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.

12. The ~~state and agency~~ ~~I~~information Resource S~~s~~ecurity P~~p~~rogram~~s~~ or Information Technology Security Program ~~and plans~~ must be responsive and adaptable to changing environments, vulnerabilities and technologies affecting state information resources.

13. The state should support and uphold the legitimate proprietary interests of intellectual property owners in accordance with applicable federal and state law.

14. Providers shall comply with the Florida Information Resource Security Policies and Standards.

(b) Implementation and maintenance of a documented on-going training program for information resource security awareness. The training program will include initial security awareness training for all new information resource users, custodians, providers, and their management and on-going reinforcement covering agency security program components and applicable security related job responsibilities. Each individual must be held accountable for his or her actions relating to information resources.

(c) A set of defined roles and responsibilities of Information Security Managers and data security administrators.

(d) Documentation of employees and providers acknowledgment and acceptance of agency's security policies, procedures, and responsibilities. An individual acknowledgement of accountability shall be included in such documentation.

(e) Clearly defined and current security responsibilities for each information resource user, custodian, provider, and his/her management.

(f) Documentation for managing access criteria ~~and privileges~~ for information resources.

(g) Current lists of information resource owners approved and maintained by the agency or secretary of the agency.

(h) Current lists of information resource users approved and maintained by the agency or secretary of the agency. Except as permitted under paragraph 60DD-2.004(1)(a), Florida Administrative Code, information resource users shall be individually identified.

(i) Current lists of information resource custodians approved and maintained by the agency or secretary of the agency.

(j) Current documented procedures for conducting background checks for positions of special trust and responsibility or positions in sensitive locations approved and maintained by the agency or secretary of the agency.

(k) An on going documented program of risk management, including risk analysis for all critical information resources, and periodic comprehensive risk analyses of all information resources. Comprehensive risk analyses shall be conducted after major changes in the software, procedures, environment, organization, or hardware.

(l) Current identification of all agency critical information resources approved and maintained by the agency's Information Security Manager (ISM). Agencies shall categorize all information and information systems in accordance with Federal Information Processing Standard 199, incorporated by reference at subsection 60DD-2.010(6), Florida Administrative Code, and Sections 119.07(3)(o) & 282.318, Florida Statutes.

(m) For all critical information resources, current documentation for implementing and maintaining auditable disaster-preparedness plans including: procedures for cross training of critical or unique skills; responsibilities and procedures for information resource custodians, owners, and users; procedures for maintaining current data on critical

information resources (including hardware, software, data, communications, configurations, staff, special forms, and supplies); and interdependencies between and among resources (both internal and external).

(n) Current documentation for executing and maintaining test scenarios for disaster-preparedness plans.

(4) Applicability.

(a) The information security policies and standards of this rule chapter apply to those entities described in Section 216.011(1)(qq), Florida Statutes. They apply to state automated information systems that access, process, or have custody of data. They apply to mainframe, minicomputer, distributed processing, and networking environments of the state. They apply equally to all levels of management and to all supervised personnel.

(b) State information security policies and standards of this rule chapter apply to information resources owned by others, such as political subdivisions of the state or agencies of the federal government, in those cases where the state has a contractual or fiduciary duty to protect the resources while in the custody of the state. In the event of a conflict, the more restrictive security measures apply.

(c) Exceptions.

1. Heads of executive agencies are authorized to exempt from the application of paragraph 60DD-2.004(2)(b), subsection 60DD-2.004(4), paragraphs 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), F.A.C., of this rule, information resources used for classroom or instructional purposes, provided the head of the agency has documented his or her acceptance of the risk of excluding these resources, and further provided that the information resources used for classroom or instructional purposes are not critical.

2. The head of an executive agency is authorized to exempt from the application of paragraph 60DD-2.004(2)(b), subsection 60DD-2.004(4), paragraphs 60DD-2.005(3)(a), 60DD-2.005(3)(b), or 60DD-2.005(4)(b), F.A.C., of this rule, stand-alone end user workstations, provided these workstations are not used to process, store, or transmit critical information resources.

(5)(a) Agency Security Program ~~and plans~~. The purpose of an agency security program ~~and plans~~ is to ensure that the security of the information resources of the agency is sufficient to reduce the risk of loss, modification or disclosure of those assets to an acceptable level. As identified in the agency's comprehensive risk analysis, the expense of security safeguards must be commensurate with the value of the assets being protected.

(b) Standard. Each agency shall develop an Information Resource Security Program that includes a documented and maintained current internal Information Resource Security Plan(s) approved by the agency Chief Information Office (CIO), and maintained by the agency's Information Security Manager (ISM). The agency security program and plan(s) shall include written internal policies and procedures for the protection of information resources, be an instrument implementing the Florida Information Resource Security Policies and Standards, be applicable to all elements of the agency, and be signed by the agency head.

(6)(a) Responsibility; Security Audits. The State Technology Office, in consultation with each agency head, is responsible for the security of the each agency's information resources and for establishing information security requirements on an agency-wide basis. To assist the State Technology Office in carrying out security responsibilities, the duties and functions which management has determined to be appropriate for each agency need to be explicitly assigned. When necessary, based on the outcome of risk analysis, to ensure integrity, confidentiality and availability of state information and resources or to investigate possible security incidents to ensure conformance this rule chapter and Florida law, the State Technology Office shall conduct or contract with a third party to conduct a security audit on any system within the State of Florida networks to determine compliance with the Florida Information Resource Security Policies and Standards. Pursuant to Section 282.318(2)(a)5., the State Technology Office shall also ensure that each agency conducts periodic internal audits and evaluations of its Information Technology Security Plan.

(b) Standard. Pursuant to Section 282.318(2)(a)1., Florida Statutes, the State Technology Office shall, in consultation with each agency head, appoint in writing an Information Security Manager (ISM) to administer the agency information resource security program ~~and plans~~ and shall prescribe the duties and responsibilities of the function for each agency.

(7)(a) Owner, Custodian, and User Responsibilities. The major objective of information resource security is to provide cost-effective controls to ensure that information is not subject to unauthorized acquisition, use, modification, disclosure, or destruction. To achieve this objective, procedures that govern access to information resources must be in place. The effectiveness of access rules depends to a large extent on the correct identification of the owners, custodians, and users of information. Owners, custodians, and users of information resources shall be identified, documented, and their responsibilities defined.

(b) Standard. Owner responsibilities. All information resources shall be assigned an owner. In cases where information resources are aggregated for purposes of ownership, the aggregation shall be at a level that assures individual accountability. The owner or his or her designated representative(s) are responsible for and authorized to:

1. Approve, access and formally assign custody of an information resources asset;

2. Determine the asset's value;

3. Specify data control requirements and convey them to users and custodians;

4. Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the agency;

5. Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data;

6. Ensure compliance with applicable controls;

7. Assign custody of information resource assets and provide appropriate authority to implement security control and procedures;

8. Review access lists based on documented agency security risk management decisions.

(c) Standard. Custodian responsibilities. Custodians of information resources, including entities providing outsourced information resources services to state agencies or other providers, must:

1. Implement the controls specified by the owner(s);

2. Provide physical and procedural safeguards for the information resources;

3. Assist owners in evaluating the cost-effectiveness of controls and monitoring; and

4. Implement the monitoring techniques and procedures for detecting, reporting and investigating incidents.

(d) Standard. User responsibilities. Users of information resources shall comply with established controls.

(8) Risk Management. Risk analysis is a systematic process of evaluating vulnerabilities and threats to information resources. Risk analysis provides the basis for risk management; i.e., assumption of risks and potential losses, or selection of cost effective controls and safeguards to reduce risks to an acceptable level. The goal of risk analysis is to determine the probability of potential risks, in order to integrate financial objectives with security objectives.

(a) Standard. Agencies shall perform or update a comprehensive risk analysis of all critical information processing systems when major changes occur and as specified in subsection 60DD-2.001(3), Florida Administrative Code. Comprehensive risk analysis results shall be presented to the State Technology Office and to the owner of the information resource for subsequent risk management.

(b) Standard. Agencies shall implement appropriate security controls determined through comprehensive risk analysis to be cost effective in the reduction or elimination of identified risks to information resources. Any delegation by the agency head of authority for risk management decisions shall be documented.

(c) Standard. The State Technology Office shall evaluate potentially useful risk analysis programs and methodologies. Only those programs and methodologies approved by the State Technology Office shall be accepted as meeting the requirements for comprehensive risk analysis as specified in paragraph 60DD-2.001(8)(a), Florida Administrative Code.

(d) Standard. Agencies shall perform a risk analysis consistent with NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, ~~is hereby~~ incorporated by reference at subsection 60DD-2.010(7), Florida Administrative Code. ~~Agencies shall perform a risk analysis consistent with Special Publication 800-30.~~

Specific Authority 282.102(2),(6),(16) FS. Laws Implemented 282.0041, 282.101, 282.318 FS. History–New _____.

60DD-2.004 Logical and Data Access Controls.

(1) Personal Identification, Authentication, and Access.

(a) Standard. Except for public web page information resources, each user of a multiple-user information resource shall be assigned a unique personal identifier or user identification. User identification shall be authenticated before access is granted.

(b) Standard. When a unique personal identifier or user identification has been assigned that user's access authorization shall be removed when the user's employment is terminated or the user transfers to a position where access to the information resource is no longer required.

(2)(a) Password Controls. Personal passwords are used to authenticate a user's identity and to establish accountability. Access passwords are used to grant access to data and may be used where individual accountability is not required. Federal Information Processing Standards Publication 112 (FIPS PUB 112) (incorporated by reference at subsection ~~Section~~ 60DD-2.010(2), Florida Administrative Code) specifies basic security criteria in the use of passwords to authenticate personal identity and data access authorization.

(b) Standard. Systems that use passwords shall conform to the federal standard contained in FIPS PUB 112. A current Password Standard Compliance Document that specifies the criteria to be met for the ten factors contained in the standard shall be maintained for all systems which use passwords.

(c) Standard: Agency Heads and Agency Chief Information Officers shall ensure that all personnel (including providers and end users who utilize State of Florida information technology resources) that have a user account on the State of Florida internal network have read and acknowledged a written password policy (or other authentication policy, if applicable) by signing through a physical or electronic process a Statement of Understanding. ~~The form shall be stored either electronically or physically in some permanent location.~~ The Statement of Understanding shall indicate that the employee has read the policy and agrees to abide by it as consideration for continued employment with the State of Florida and that violation of password or other authentication policies may result in dismissal. Agency Heads and Chief Information Officers shall also ensure that information technology professionals enforce the parts of the policy within the scope of their capability, and that periodic compliance audits are performed.

(3) Standard. Authentication Controls. All agency authentication controls shall ensure that information is not accessed by unauthorized persons and that information is not altered by unauthorized persons in a way that is not detectable by authorized users.

(4) Standard. Access to Software and Data. Controls shall ensure that users of information resources cannot access stored software or system control data unless they have been authorized to do so.

(5) Encryption.

(a) Standard. Activities storing or transmitting confidential or exempt information shall require encryption processes approved by the State Technology Office if necessary to ensure that the information remains confidential. Individual users must use State Technology Office approved encryption products and processes for sending an encrypted e-mail, encrypting a desktop work file, protecting a personal private key or digital certificate, or encrypting a saved e-mail. Key escrow and Key recovery processes must be in place, and verified prior to encryption of any confidential or exempt agency data. Federal Information Processing Standard (FIPS) Pub 140-2, May 25, 2001 (http://csrc.nist.gov/cryptval/140-2.htm) ~~is hereby adopted and~~ incorporated by reference at subsection 60DD-2.010(3), Florida Administrative Code.

(b) Standard. Encryption keys should not be stored on the same electronic storage device as the information that has been encrypted using the keys. Access to encryption keys should be restricted to authorized users and authorized processes using an access control mechanism.

(c) Standard. Remote administration of hardware, software, or applications should be performed over an encrypted communications session consistent with the Florida Information Resource Security Policies and Standards.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.006 Network Security.

Networking, including distributed processing, concerns the transfer of information among users, hosts, servers, applications, voice, video and intermediate facilities. During transfer, data is particularly vulnerable to unintended access or alternation.

(1) Network Controls, General.

(a) Standard. Network resources used in the access of confidential or exempt information shall assume the sensitivity level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

(b) Standard. All network components under state control must be identifiable and restricted to their intended use.

(2)(a) Security at Network Entry and Host Entry. State owned or leased network facilities and host systems are state assets. Their use must be restricted to authorized users and purposes. ~~Where public users are authorized access to networks or host systems, these public users as a class must be clearly identifiable and restricted to only services approved for public functions.~~ State employees who have not been assigned a user identification code and means of authenticating their identity to the system are not distinguishable from public users and must not be afforded broader access.

1. User identification and authentication (e.g., password) or

(b) Standard. Owners of information resources served by networks shall prescribe sufficient controls to ensure that access to network services and host services and subsystems are restricted to authorized users and uses only. These controls shall selectively limit services based upon:

2. Designation of other users, including the public where authorized, as a class (e.g., public access through dial-up or public switched networks), for the duration of a session.

(c) Third Party Connections.

1. Agency third party connection agreements shall determine the responsibilities of the third party, including approval authority levels and all terms and conditions of the agreement.

2. All agency third party network connections must meet the requirements of the Florida Information Resource Security Policies and Standards. Blanket access is prohibited. Service provided over third party network connections is limited to services, devices and equipment needed.

(d) Internet connectivity. Internet connectivity is allowable only if the applicable service agreement permits.

(e) Any external individual or entity needing access to the State's secure network inside state firewalls shall do so through Universal Access Service, Route Transport Service Extranet, Virtual Private Network or Frame Relay Network Extranet.

(f) Audits. Each agency shall audit third party network connections by conducting Security Vulnerability Assessments.

(3)(a) Application-level Security.

(b) Standard. Network access to an application containing confidential or exempt data, and data sharing between applications, shall be as authorized by the application owners and shall require authentication.

(4) Data and File Encryption.

(a) Security through encryption depends upon both of the following:

1. Proper use of an approved encryption methodology, and

2. Only the intended recipients holding the encryption key-variable (key) for that data set or transmission.

(b) Standard. While in transit, information which is confidential, exempt or information which in and of itself is sufficient to authorize disbursement of state funds shall be encrypted if sending stations, receiving stations, terminals, and relay points are not all under positive state control, or if any are operated by or accessible to personnel who have not been authorized access to the information, except under the following conditions:

1. The requirement to transfer such information has been validated and cannot be satisfied with information which has been sanitized, and

2. The agency head, or the designated official if the agency head has delegated authority for risk management decisions, has documented acceptance of the risks of not encrypting the information based on evaluation of the costs of encryption against exposures to all relevant risks.

(c) Standard. For systems employing encryption as required by paragraph 60DD-2.006(4)(b), Florida Administrative Code, procedures shall be prescribed for secure handling, distribution, storage, and construction of Data Encryption Standard (DES) key variables used for encryption and decryption. Protection of the key shall be at least as stringent as the protection required for the information encrypted with the key.

(d) Standard. Confidential or exempt data or information shall be encrypted pursuant to the Advanced Encryption Standard or "AES" defined in Federal Information Processing Standard Publication 197, ~~hereby~~ incorporated by reference at subsection 60DD-2.010(5), Florida Administrative Code, or the Triple Data Encryption Standard known as "Triple DES" or "3DES". Legacy systems not supporting the "AES" or "3DES" shall not store confidential or exempt data or information, but may use the federal Data Encryption Standard or "DES" defined in Federal Information Processing Standard Publication (FIPS PUB 46-3) (incorporated by reference at subsection 60DD-2.010(1), Florida Administrative Code) for other data or information as necessary.

(e) Standard. A minimum requirement for digital signature verification shall be in accordance with the Federal Information Processing Digital Signature Standard, (FIPS PUB 186-2), ~~which is hereby~~ incorporated by reference at subsection 60DD-2.010(4), Florida Administrative Code.

(5)(a) Remote Access.

(b) Standard. For services other than public access, users of state dial-up services shall be positively and uniquely identifiable and their identity authenticated (e.g., by password) to the network accessed and to the systems being accessed.

(6)(a) Security Alerts

(b) Standard. The State Technology Office will maintain the capability to monitor the Internet and appropriate global information security resources for any abnormalities or threats present on the Internet, including the detection of backdoors or hardware or software that is intentionally included or inserted in a system for a harmful purpose. Such abnormalities or threats will then be translated into Information Security Alerts and provided to state agencies. In response to each Information Security Alert, agencies shall log corrective actions and to implement the recommended remediation actions contained in the Information Security Alerts within the alert's recommended time frame. Agencies shall notify the State Technology Office in writing when remediation is complete. The State Technology Office shall verify that agencies are implementing the requisite Information Security Alert remediation actions.

(c) Standard. The State Technology Office shall keep a log of all Information Security Alerts sent. The log shall contain tracking information on all formats of alerts issued, and the associated actions taken as reported by each agency. The State Technology Office shall report any non-compliance of with Information Security Alerts to applicable agency heads.

(7)(a) Virus Detection and Prevention.

(b) Standard. All State computers and systems must have anti-virus software that provides protection to computer systems and media from computer virus intrusion, provides detection of computer viruses on an infected computer system or media, and provides for recovery from computer virus infection. Anti-virus software shall be installed and scheduled to run at regular intervals. Real-time scanning shall be enabled. The anti-virus software and the virus pattern files must be kept current. Virus-infected computers or systems must be removed from the network until they are verified as virus-free. This rule applies to State of Florida computers that are personal computer ("PC")-based or utilize PC-file directory sharing, including desktop computers, laptop computers, servers (including domain controllers, proxy, ftp, file and print, etc.), and any PC-based equipment such as firewalls, intrusion detection systems (IDS), gateways, routers, and wireless devices.

(c) Standard. Each State agency is responsible for creating procedures that ensure anti-virus software is run at regular intervals and that computers and systems are verified as virus-free.

(8) Mobile Device Security.

(a) Standard. State agencies shall prepare written policies and procedures for mobile device use incorporating core security measures consistent with the Florida Information Resource Security Policies and Standards. Agencies shall, consistent with the capability of the device and its software, utilize a secure operating system offering secure logon, file level security, and data encryption. Agencies shall enable a strong password for mobile device use consistent with paragraphs 60DD-2.004(2)(a)-(c), Florida Administrative Code. Agencies mobile devices shall utilize anti-virus software in consistent with paragraph 60DD-2.0069( )(b), Florida Administrative Code.

(b) Standard. Agencies shall asset tag or engrave laptops, permanently marking (or engraving) the outer case of the laptop with the agency name, address, and phone number or utilizing a metal tamper resistant commercial asset tag.

(c) Standard. Agencies shall register mobile devices with the manufacturer and retain the registration correspondence and any applicable serial numbers in the agency's records.

(9) Wireless Connectivity.

(a) Wireless security is essential to:

1. Safeguard security of the State's network systems and data.

2. Prevent interference between different agency implementations and other uses of the Wireless spectrum.

3. Ensure that a baseline level of connection service quality is provided to a diverse user community.

(b) Standard. A site survey shall be conducted prior to wireless implementation that includes identification of security risks and threats.

(c) Standard. If VPN services are used, split tunnel mode shall be disabled when connected to any wireless network.

(d) Standard. Strong mutual user authentication shall be utilized.

(e) Standard. When passing wireless traffic over public networks use of strong encryption or utilization of State of Florida sanctioned VPNs shall be used.

(f) Standard. The SSID name shall be changed from the default and administrative passwords shall be changed every 180 days.

(g) Standard. Security features of the Access Point vendors shall be enabled.

(h) Standard. Access points shall be Wi-Fi compliant pursuant to IEEE Standard 802.11, ~~which is hereby~~ incorporated by reference at subsection 60DD-2.010(17), Florida Administrative Code. Standard 802.11 specifies medium access and physical layer specifications for 1 Mbps and 2 Mbps wireless connectivity between fixed, portable, and moving stations within a local area.

(i) Standard. IP forwarding shall be disabled on all wireless clients.

(j) Standard. Master keys shall be changed annually, and key rotation schemes shall be changed at least once every 15 minutes.

(k) Standard. Theft or loss of a wireless-enabled device shall be reported to the agency Information Security Manager in order to retire the device's credentials.

(l) Standard. Wireless devices shall not be connected simultaneously to another wired or wireless network other than standard utilization of a commercial carrier signal.

(m) Standard. Wireless devices shall be password protected and must automatically time out in 15 minutes or less.

(n) Standard. Wireless devices having the features of personal firewalls and anti-virus capability shall be enabled.

(10) Web Servers and Network Servers.

(a) Security of Web Servers providing Public Internet access is essential to address:

1. Proper configuration and operation of the host servers to prevent inadvertent disclosure or alteration of confidential or exempt information.

2. Preventing compromise of the host server

3. Users unable to access the Web site due to a denial of service.

(b) Standard. Agencies shall secure network and public web servers consistent with the Carnegie Mellon Software Engineering Institute's Security Improvement Module, "Securing Network Servers" incorporated by reference at subsection 60DD-2.010(19), Florida Administrative Code, and NIST Guidelines on Securing Public Web Servers, Special Publication 800-44, ~~which are both hereby~~ incorporated by reference at subsection 60DD-2.010(10), Florida Administrative Code.

(c) Standard. Network Servers housed in the State Technology Office, Shared Resource Center shall be subject to a Security Vulnerability Assessment prior to connection to the State Technology Internal Network.

(11) Electronic Mail Security.

(a) Standard. Agencies shall utilize NIST Guidelines on Electronic Mail Security, Special Publication 800-45, ~~is hereby~~ incorporated by reference at subsection 60DD-2.006(11), Florida Administrative Code, as a standard for electronic mail security.

(12) Firewalls.

(a) Standard. Agencies shall utilize NIST Guidelines on Firewalls and Firewall Policy, Special Publication 800-41, ~~is hereby~~ incorporated by reference at subsection 60DD-2.010(9), Florida Administrative Code, as a standard for firewalls.

(13) Patching of Network Servers, Workstations and Mobile Devices.

(a) Standard. Agencies shall utilize NIST Procedures for Handling Security Patches, Special Publication 800-40, ~~is hereby~~ incorporated by reference at subsection 60DD-2.010(8), Florida Administrative Code, as a standard for patching of network servers, workstations and mobile devices.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.007 Backup and Disaster Recovery.

(1)(a) Backing up of Data. On-site backup is employed to have readily available current data in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted, without having to resort to reentry from data sources, i.e., other electronic or hard copy records. Off-site backup or storage embodies the same principle but is

designed for longer term protection in a more sterile environment, requires less frequent updating, and is provided additional protection against threats potentially damaging to the primary site and data.

(b) Standard. Data and software essential to the continued operation of critical agency functions shall be backed up. The security controls over the backup resources shall be as stringent as the protection required of the primary resources.

(2) Contingency Planning. Disaster-Preparedness Plans, as described in subparagraph 60DD2.001(2)(a)36.~~(jj)~~, Florida Administrative Code, specify actions management has approved in advance to achieve each of three objectives. The emergency component assists management in identifying and responding to disasters so as to protect personnel and systems and limit damage. The backup and disaster recovery plan specifies how to accomplish critical portions of the mission in the absence of a critical resource such as a computer. The overall Disaster-Preparedness Plan directs recovery of full mission capability.

(a) Standard. All information resource owner, custodian, and user functions identified as critical to the continuity of governmental operations shall have written and cost effective disaster-preparedness plans to provide for the prompt and effective continuation of critical state missions in the event of a disaster.

(b) Standard. Disaster-preparedness plans as required by paragraph 60DD-2.007(2)(a), Florida Administrative Code, shall be tested at least annually.

Specific Authority 282.102(2),(6),(16) FS. Law Implemented 252.365, 282.318 FS. History–New _____.

60DD-2.008 Personnel Security and Security Awareness.

(1)(a) End User Requirements, General.

(b) Standard. Every employee shall be held responsible for information resources security to the degree that his or her job requires the use of information resources.

(2)(a) Positions of Special Trust or Responsibility or in Sensitive Locations. Individual positions must be analyzed to determine the potential vulnerabilities associated with work in those positions. Agencies shall prepare written procedures for personnel in positions of special trust or having access to sensitive locations. Agencies shall utilize ISO/EC 17799-2000(E), 8.6.3, Information Handling Procedures~~:~~ ~~is hereby~~ incorporated by reference at subsection 60DD-2.010(15), Florida Administrative Code, as a guide for development of procedures.

(b) Standard. Agencies shall establish procedures for reviewing data processing positions that are designated as special trust or are in sensitive locations.

(c) Standard. Agencies shall conduct background investigations for personnel in positions of special trust or having~~e~~ access to sensitive locations as set forth in Sections 110.1127 and 435.04, Florida Statutes.

(3) Security Awareness and Training. An effective level of awareness and training is essential to a viable information resource security program.

(a) Standard. Agencies shall provide an ongoing awareness and training program in information security and in the protection of state information resources for all personnel whose duties bring them into contact with critical state information resources. Security training sessions for these personnel shall be on going. Agencies shall utilize NIST Building an Information Security Technology Awareness and Training Program, Special Publication 800-50, ~~is hereby~~ incorporated by reference at subsection 60DD-2.010(12), Florida Administrative Code, as a guide for development of such programs.

(b) Standard. Awareness and training in security shall not be limited to formal training sessions, but shall include on-going briefings and continual reinforcement of the value of security consciousness in all employees whose duties bring them into contact with critical state information resources.

(c) Standard. Departments shall apply appropriate sanctions against any employee who fails to comply with its security policies and procedures.

Specific Authority 282.102(2),(16) FS. Law Implemented 282.318 FS. History–New _____.

60DD-2.009 Systems Acquisition, Disposal, Auditing, and Reporting.

(1)(a) Systems Acquisition. Major system development decisions must be based on consideration of security and audit requirements during each phase of life cycle development.

(b) Standard. Appropriate information security and audit controls shall be incorporated into new systems. Each phase of systems acquisition shall incorporate corresponding development or assurances of security and auditability controls.

(2)(a) Systems Disposal. Device and media controls. Agencies shall implement policies and procedures that govern the receipt and removal of hardware and electronic media/devices that contain confidential or exempt information into and out of a facility, and the movement of these items within the facility.

(b) Implementation specifications: Agencies shall implement policies and procedures to address the final disposition of confidential or exempt information, and the hardware or electronic media on which it is stored.

(c) Media and Devices re-use or disposal. Agencies shall implement procedures for removal of confidential or exempt information from electronic media before the media are made available for re-use or disposal in accordance with ISO 17799-2000(E), 7.2.6, Secure disposal or re-use of equipment, and 8.6.2, Disposal of Media, incorporated by reference at subsection 60DD-2.010(15), Florida Administrative Code, and NIST Security Considerations in the Information System

Development Life Cycle, Special Publication 800-64, ~~which are hereby~~ incorporated by reference at subsection 60DD-2.010(13), Florida Administrative Code.

(3) Audits. The establishment and maintenance of a system of internal control is an important management function. Internal audits of information resource management functions, including security of data and information technology resources in accordance with paragraph 60DD-2.001(6)(a), Florida Administrative Code, are an integral part of an overall security program. The frequency, scope, and assignment of internal audits for security of data and information technology resources should be established to ensure that agency management has timely and accurate information concerning functions management is responsible to perform.

(a) Standard. An internal audit of the agency information security function shall be performed annually or when there are major system changes, or as directed by the head of the department.

(b) Standard. Automated systems which process confidential or exempt ~~sensitive~~ information must provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, or effect the release of the information.

(4) Incident Reporting.

(a) Continuous analysis of trends and types of security incidents and breaches is important to the integrity of agency and state information resource security programs. Security incident reporting provides a basis for a continuing evaluation of agency and state information security postures. The objective of such analysis is to refine security rules, policies, standards, procedures, guidelines, and training programs to assure their continued effectiveness and applicability.

(b) Standard. Security incidents and breaches shall be promptly investigated and reported to the appropriate authorities.

(c) Standard. The State Technology Office shall provide analysis and centralized reporting of trends and incidents to agencies, and shall initiate appropriate changes to state policies, rules, standards, guidelines, training programs, or statutes.

(d) Standard. Response teams. Each agency shall create an organized team to address cyber alerts and responses. Each team shall include at least one individual with expertise from the agency's legal, human resources, inspector general and information technology areas, as well as the Chief Information Officer and the Information Security Manager of the agency. The team shall report computer security incidents to the State Technology Office's Office of Information Security, convene as required upon notification of a reported computer security incident, respond to activities that may interrupt the information technology services of the area for which the team is responsible during duty and non-duty hours, classify, document and investigate agency security incidents, and maintain an awareness of and implement procedures for effective response to computer security incidents. The team shall provide regular reports to the agency's Chief Information Officer and shall follow the direction of the Chief Information Officer during incident response activities.

Specific Authority 282.102(2),(16) FS. Law Implemented 281.301, 282.318 FS. History–New _____.

60DD-2.010 Standards Adopted.

(1) Federal Information Processing Standard Publication Number 46-3 – Data Encryption Standard, October 25, 1999, is hereby incorporated by reference.

(2) Federal Information Processing Standard Publication Number 112 – Password Usage, May 30, 1985, is hereby incorporated by reference.

(3) Federal Information Processing Standard Publication Number 140-2, Security Requirements for Cryptographic Modules, is hereby incorporated by reference.

(4) Federal Information Processing Standard Publication Number 186-2, Digital Signature Standard, is hereby incorporated by reference.

(5) Federal Information Processing Standard Publication Number 197, Advanced Encryption Standard, is hereby incorporated by reference.

(6) Federal Information Processing Standard Publication Number 199 – Standards for Security Categorization of Federal Information and Information Systems, December 5, 2003, is hereby incorporated by reference.

(7) NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, is hereby incorporated by reference.

(8) NIST Procedures for Handling Security Patches, Special Publication 800-40, is hereby incorporated by reference.

(9) NIST Guidelines on Firewalls and Firewall Policy, Special Publication 800-41, is hereby incorporated by reference.

(10) NIST Guidelines on Securing Public Web Servers, Special Publication 800-44, is hereby incorporated by reference.

(11) NIST Guidelines on Electronic Mail Security, Special Publication 800-45, is hereby incorporated, is hereby incorporated by reference.

(12) NIST Building an Information Security Technology Awareness and Training Program, Special Publication 800-50 is hereby incorporated by reference.

(13) NIST Security Considerations in Information System Development Life Cycle, Special Publication 800-64, is hereby incorporated by reference.

(14) Copies of these standards are available for downloading from the National Institute of Standards and Technology at www.nist.gov or by writing orders@ntis.gov or:

United States Department of Commerce

National Technical Information Service

5285 Port Royal Road

Springfield, Virginia 22161

(15) Section 7.2.6 ("Secure Disposal or Re-Use of Equipment"), Section 8.6.2 ("Disposal of Media"), and Section 8.6.3 ("Information Handling Procedures") of International Organization for Standardization ISO/IEC Standard 17799 are ~~is~~ hereby incorporated by reference.

(16) Copies of these sections of the ~~this~~ standard are available from the American National Standards Institute at www.ansi.org or at info@ansi.org or by writing:

American National Standards Institute

25 West 43rd Street, 4th Floor

New York, New York 10036

(17) Institute of Electrical and Electronics Engineers~~, Inc.,~~ Standard 802.11 is hereby incorporated by reference.

(18) Copies of this standard are available from the Institute of Electrical and Electronics Engineers, at www.ieee.org or at ieeeusa@ieee.org or by writing:

Institute of Electrical and Electronic Engineers~~, Inc.~~

1828 L. Street, N. W., Suite 1202

Washington, D. C. 20036-5104

(19) The Carnegie Mellon Software Engineering Institute's Security Improvement Module, "Securing Network Servers," is hereby incorporated by reference.

(20) Copies of this security improvement module are available from the Carnegie Mellon Software Engineering Institute at www.cert.org or at webmaster@cert.org or by writing:

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, Pennsylvania 15213-3890

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Division of Florida Land Sales, Condominiums and Mobile Homes

RULE NOS.:	RULE TITLES:
61B-45.009	Computation of Time; Service by Mail
61B-45.048	Claim for Costs and Attorney's Fees

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rules published in Vol. 30, No. 12, March 19, 2004, issue of the Florida Administrative Weekly, in accordance with subparagraph 120.54(3)(d)1., Florida Statutes. The changed rule provisions shall now read as follows:

61B-45.009 Computation of Time; Service by Mail.

(2) Additional Time After Service By Mail. Unless otherwise ordered by the arbitrator, during the pendency of a case, when a party is required or permitted by these rules or by order of the arbitrator to do an act within a prescribed period after the service of a document and that document is served by regular U.S. mail, five days shall be added to the prescribed period. No additional time shall be added to the prescribed period if service is made by hand, facsimile transmission, or other electronic transmission. No additional time is added for filing a motion for rehearing that must be filed (e.g., received by the agency) within 15 days of entry of a final order, or a motion for costs and attorney's fees that must be filed within 45 days of entry of the final order as required by Rule 61B-45.048, Florida Administrative Code unless an appeal for trial de novo has been timely filed in the courts. Also, no additional time is added by operation of this rule for the filing of a complaint for trial de novo which must be filed in the courts within 30 days of the date of rendition of a final arbitration order as required by Section 718.1255(4)(k), Florida Statutes.

61B-45.048 Claim for Costs and Attorney's Fees.

(2) A prevailing party seeking an award of costs and attorney's fees shall file a motion seeking the award not later than 45 days after rendition of the final order, except that if an appeal by trial de novo has been timely filed in the courts, a motion seeking prevailing party costs and attorney's fees must be filed within 45 days following the conclusion of that appeal and any subsequent appeal. The motion is considered "filed" when it is received by the division. The motion shall:

(5) A final order on the motion for attorney's fees or costs shall be entered in the manner and within the time prescribed by Rule 61B-45.043, Florida Administrative Code. In determining a reasonable hourly fee and a reasonable total award of costs and attorney's fees, the arbitrator is not required to conduct any hearing or proceedings or to seek or consider expert advice or testimony.

(7) The prevailing party in a proceeding brought pursuant to Section 718.1255, Florida Statutes, is entitled to an award of reasonable costs and attorney's fees. A prevailing party is a party that obtained a benefit from the proceeding and includes a party where the opposing party has voluntarily provided the relief requested in the petition, in which case it is deemed that the relief was provided in response to the filing of the petition. Where a respondent has provided the relief sought by the petitioner prior to the filing of the petition and service on the respondent of the order requiring answer and copy of the petition, the petitioner under these circumstances is not deemed to be a prevailing party and is not entitled to an award of reasonable costs and attorney's fees. The factors to be considered by the arbitrator in determining a reasonable attorney's fees include the following:

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Architecture and Interior Design

RULE NO.:	RULE TITLE:
61G1-23.040	Responsible Supervising Control Over Design Practice in the Interior Designer's Office

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rule, as noticed in Vol. 29, No. 28, July 11, 2003, Florida Administrative Weekly has been withdrawn.

DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION

Board of Architecture and Interior Design

RULE NOS.:	RULE TITLES:
61G1-26.001	Individual Licensee Responsibilities
61G1-26.002	Business Responsibilities

NOTICE OF WITHDRAWAL

Notice is hereby given that the above rules, as noticed in Vol. 29, No. 35, August 29, 2003, Florida Administrative Weekly have been withdrawn.

DEPARTMENT OF ENVIRONMENTAL PROTECTION

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Department of Environmental Protection are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."

DEPARTMENT OF FINANCIAL SERVICES

Division of Workers' Compensation

RULE NO.:	RULE TITLE:
69L-7.020	Florida Workers' Compensation Health Care Provider Reimbursement Manual

NOTICE OF CHANGE

Notice is hereby given that the following changes have been made to the proposed rule in accordance with subparagraph 120.54(3)(d)1., F.S., published in Vol. 30, No. 16, April 16, 2004, of the Florida Administrative Weekly.

These changes are being made to address concerns expressed at the public hearing held on May 11, 2004, Page 4, subparagraph b.(1) of the incorporated document, Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition is changed to read as follows:

(1) Reimbursement shall be made to a Florida health care provider for medical services. After applying the appropriate reimbursement guidelines contained in this manual, a carrier shall reimburse a provider the agreed upon contract price (whether agreed upon prior to rendering service(s) or upon submission of the bill) or the maximum reimbursement allowance in the appropriate schedule pursuant to Section 440.13(12)(a), Florida Statutes (F.S.). (See Section XI, General Instructions, Maximum Reimbursement Allowances.)

Page iii, of the incorporated document, Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition is amended as follows:

The five character codes included in the Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition are obtained from Current Procedural Terminology (CPT®), copyright 2003 by the American Medical Association (AMA). CPT is developed by the AMA as a listing of descriptive terms and five character identifying codes and modifiers for reporting medical services and procedures performed by physicians.

The responsibility for the content of the Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition is with the State of Florida Division of Workers' Compensation and no endorsement by the AMA is intended or should be implied. The AMA disclaims responsibility for any consequences or liability attributable or related to any use, nonuse or interpretation of information contained in The Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition. No fee schedules, basic unit values, relative value guides, conversion factors or scales are included in any part of CPT. Any use of CPT outside of the Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition should refer to the most current Current Procedural Terminology which contains the complete and most current listing of CPT codes and descriptive terms. Applicable FARS/DFARS apply.

~~CPT codes, descriptions and material only are copyright 2003 American Medical Association. All Rights Reserved. No fee schedules, basic units, relative values or related listings are included in CPT. The American Medical Association assumes no liability for the data contained or not contained herein.~~

This product includes CPT, which is commercial technical data and/or computer databases and/or commercial computer software and/or commercial software documentation, as applicable which were developed exclusively at private expense by the American Medical Association, 515 North State Street, Chicago, Illinois 60610. U.S. Government rights to use, modify, reproduce, release, perform, display, or disclose these technical data and/or computer data bases and/or computer software and/or computer software documentation are subject to the limited rights restrictions of DFARS 252.227-7015(b)(2) (June 1995) and/or subject to the restrictions of DFARS 227.7202-1(a) (June 1995) and DFARS 227.7202-3(a) (June 1995), as applicable for U.S. Department of Defense procurements and the limited rights restrictions of FAR 52.227-14 (June 1987) and/or subject to the restricted rights provisions of FAR 52.227-14 (June 1987) and FAR

52.227-19 (June 1987), as applicable, and any applicable agency FAR Supplements, for non-Department of Defense Federal procurements.

The column labels on pages 114-117 of the incorporated document, Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition are amended as follows:

D-~~CPT~~ Code

The column labels on pages 118-120 of the incorporated document, Florida Workers' Compensation Health Care Provider Reimbursement Manual, 2004 Second Edition are amended as follows:

J-~~CPT~~ Code

The remainder of the rule reads as previously published.

Section IV
Emergency Rules

BOARD OF TRUSTEES OF THE INTERNAL IMPROVEMENT TRUST FUND

Pursuant to Chapter 2003-145, Laws of Florida, all notices for the Board of Trustees of the Internal Improvement Trust Fund are published on the Internet at the Department of Environmental Protection's home page at http://www.dep.state.fl.us/ under the link or button titled "Official Notices."

STATE BOARD OF ADMINISTRATION

RULE TITLES:	RULE NOS.:
Reimbursement Contract	19ER04-1 (19-8.010)
Insurer Reporting Requirements	19ER04-2 (19-8.029)

SPECIFIC REASONS FOR FINDING AN IMMEDIATE DANGER TO THE PUBLIC, HEALTH, SAFETY OR WELFARE: The 2004 Legislature passed CS/CS/CS/CS for SB 2488 on Friday, April 30, 2004. This legislation affects the Reimbursement Contract as a whole and specifically impacts options available in the Contract. The Contract (and selected options) must be signed and returned to the Florida Hurricane Catastrophe Fund (FHCF) prior to the June 1, 2004, commencement of the hurricane season. The legislation also affects the participating insurer's exposure reporting requirements and a proof of loss form. Given the short time frame in which these documents must be reviewed, options chosen and returned to the FHCF and the imminent onset of the 2004 hurricane season, emergency rulemaking is necessary.

REASONS FOR CONCLUDING THAT THE PROCEDURE USED IS FAIR UNDER THE CIRCUMSTANCES: Prior to the passage of the law, the FHCF placed a notice on its website that the Advisory Council was holding an emergency meeting, by conference call, to discuss the need for emergency rules should the pending legislation become law. The meeting, which was open to the public, was noticed on the FHCF website, and a notice was mailed to every person or entity on the FHCF's mailing list. In addition, the proposed emergency rules and the incorporated forms were placed on the website.

SUMMARY OF THE RULE: Rule 19ER04-1, F.A.C., is titled "Reimbursement Contract". Paragraph (10) of this rule incorporates the reimbursement contract for the 2004-2005 contract year that participating insurers must sign and return to the FHCF by June 1, 2004. Since the reimbursement contract must be amended to reflect those legislative changes, paragraph (10) of this rule refers to the "amended" reimbursement contract and states that this amended contract is incorporated by reference into this "emergency" rule. The changes made to the contract are summarized as follows: deductible buy-back and excess policies that require individual ratemaking have been excluded, additional living expense (ALE) provisions have been re-defined, the definition of "losses" has been amended, the word "audit" has been replaced with examination, the retention multiple has been reset, the prohibition against an insurer receiving reimbursements in excess of 100% has been stricken, information regarding the transitional option provided in the legislation has been provided and a new schedule has been added to allow for the selection of the option.

Rule 19ER04-2, F.A.C., is titled "Insurer Reporting Requirements". Paragraphs (4)(f) and (5)(c) and (d) have been amended to include the words "amended", the new revision dates for forms referenced and incorporated therein, and the prohibition against an insurer receiving reimbursements in excess of 100% has been stricken. The incorporated forms that require amendment to reflect the changes made by CS/CS/CS/CS for SB 2488 are Form FHCF-D1A (2004 Data Call) and the FHCF-L1B (Proof of Loss Report). The changes made in these forms can be summarized as follows: deductible buy-back and excess policies have been excluded, additional living expense (ALE) provisions have been re-defined, the definition of "losses" has been amended, the word "audit" has been replaced with examination, and the prohibition against an insurer receiving reimbursements in excess of 100% has been stricken.

THE PERSON TO BE CONTACTED REGARDING THE EMERGENCY RULE IS: Jack E. Nicholson, Senior FHCF Officer, Florida Hurricane Catastrophe Fund, State Board of Administration, Tallahassee, Florida

THE FULL TEXT OF THE EMERGENCY RULE IS:

19ER04-1 Reimbursement Contract.

(1) through (9) No changes.

(10) The amended reimbursement contract for the 2004-2005 contract year required by Section 215.555(4), Florida Statutes, which is called Form FHCF-2004K – "Reimbursement Contract" or "Contract" between (name of insurer) (the "Company")/NAIC #( ) and The State Board of Administration of the State of Florida ("SBA") which