CHAPTER 71A-1
SECURITY POLICIES AND STANDARDS

71A-1.001 Purpose and Scope.

(1) Chapter 71A-1, F.A.C., shall be known as the Florida Information Technology Resource Security Policies and Standards.

(2) The information security standards of this rule chapter apply to executive branch agencies as provided in Title IV, Florida Statutes.

(3) The information security policies and standards of this rule chapter apply equally to all levels of management and to all members of the workforce.

(4) The State of Florida government information technology resources, data, and information are valuable assets to its citizens. The confidentiality, integrity, and availability of those resources must be protected. Data and resources must be reliable, and must be available to those who are authorized to use them.

(5) The purposes of the Florida Information Technology Resource Security Standards are to:

(a) Document a framework of information security best practices for state agencies in order to safeguard the confidentiality, integrity, and availability of Florida government data and information technology resources.

(b) Define minimum standards to be used by state agencies to categorize information and information technology resources based on the objectives of providing appropriate levels of information security according to risk levels.

(c) Define minimum management, operational and technical security controls to be used by state agencies to secure information and information technology resources.

(6) State agencies shall use these standards as the minimum security requirements for information and information technology resources.

(7) Nothing in this rule chapter shall be construed as limiting the access of the Auditor General to agency records, systems, or networks in the performance of a properly authorized audit or examination pursuant to Chapters 11 and 119, F.S.

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

(9) For guidance the State of Florida will follow Federal Information Processing Standards (FIPS) and National Institute of

Standards and Technology (NIST) standards and guidelines implemented as a result of the Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. § 3541, et seq.). The Agency for Enterprise Information Technology (AEIT) Office of Information Security (OIS) will assist agencies by publishing guidelines and templates to be used by agencies when implementing these rules.

(10) Heads of executive agencies may find it necessary to employ compensating security controls when the agency is unable to implement a security standard or the standard is not cost-effective due to the specific nature of a system or its environment. After the agency analyzes the issue, a compensating control may be employed if the agency documents the analysis results and senior management documents the acceptance of the risk associated with employing the compensating control. All related documentation shall be retained by the agency Information Security Manager. This documentation is confidential, pursuant to Section 282.318, F.S., except that such information shall be available to the Auditor General and the Agency for Enterprise Information Technology.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.002 Definitions.

(1) Access – the ability to acquire, read, write, or delete data or information; make use of an information technology resource; enter a room or facility.

(2) Access control – the enforcement of specified authorization rules based on user or system authentication.

(3) Access point – a station that transmits and receives data (for example, a wireless access point).

(4) Accountability – the principle stating that a specific action is traceable to a unique individual.

(5) Agency worker – see Worker.

(6) Agency-approved software – software that has been reviewed and deemed acceptable by the agency for use with agency information technology resources.

(7) Agency-managed device – a device that is not owned by the agency, but that is declared by the device owner and accepted by the agency to be compliant with agency standard configurations.

(8) Anti-malware software – software that detects and removes malicious software from a computer or network stream.

(9) Application – information resources designed to satisfy a specific set of user requirements.

(10) Application development life cycle (ADLC) – a set of procedures to guide the development and modification of production application software and data items. A typical ADLC includes design, development, quality assurance, acceptance testing, maintenance, and disposal (also known as System Development Life Cycle – SDLC).

(11) Application development team – the entire set of people responsible for planning, designing, developing, installing, and maintaining applications. The roles represented include project managers, analysts, computer programmers, database administrators, data administrators, system administrators, network administrators, etc.

(12) Application owner – the business unit that requested the application be developed and/or purchased; the individual (usually a manager) from the business unit(s) for which an application is acquired who has responsibility and authority to make decisions related to the application, such as requirements, deliverable approvals, access, etc.

(13) Application security review – an evaluation of an application's security requirements and associated controls (planned or implemented) with the goal of determining if controls are sufficient to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

(14) Audit logs – documentation of activity within a system incorporating, at a minimum, date, time, action, and user account associated with the action.

(15) Authentication – the process of verifying that a user, process, or device is who or what it purports to be. Techniques for authentication fall into categories as follows:

(a) Something the user knows, such as a password or PIN;

(b) Something the user has, such as a smartcard or ATM card; and

(c) Something that is part of the user, such as a fingerprint, voice pattern or retinal scan.

(16) Authorization – official or legal permission or approval.

(17) Availability – the principle that authorized users have timely and reliable access to information and information technology resources.

(18) Breach – unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.

(19) Chief Information Officer – the person appointed by the agency head that coordinates and manages the agency information technology functions and responsibilities.

(20) Compensating Control – a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control that provides an equivalent or greater level of protection for an information system and the information processed, stored, or transmitted by that system.

(21) Complex password – a password that is at least eight characters and is comprised of at least three of the following categories: uppercase English letters; lowercase English letters, numbers 0-9, and non-alphanumeric characters.

(22) Comprehensive risk assessment – the risk analysis required to be conducted by agencies every three years, in accordance with Section 282.318, F.S.

(23) Computer user – any authorized entity who uses information technology resources (interchangeable with User).

(24) Confidential information and/or confidential data – information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule.

(25) Confidentiality – the principle that information is accessible only to those authorized.

(26) Continuity of Operations Plan (COOP) – the documented plan detailing how the agency will respond to incidents that could jeopardize the organization's core mission pursuant to Section 252.365, F.S.

(27) Critical information resources – the resources determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have severe or catastrophic adverse effect.

(28) Cryptography – the discipline that embodies the principles and methods for the transformation of data in order to hide semantic content, prevent unauthorized use, or prevent undetected modification. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

(29) Data store – a collection of information organized so it can be accessed, managed, and updated.

(30) Degaussing – a method of bulk erasing data from magnetic media. Degaussing demagnetizes the disk such that all data stored on the disk is permanently destroyed.

(31) Demilitarized Zone (DMZ) – physical or logical sub-network or computer host that provides an additional layer between the Internet and an organization's internal network so that external parties only have access to devices in the DMZ rather than the internal network.

(32) Development infrastructure – a technical environment that is used for design, development, and/or piloting of new technical capabilities or applications. The development infrastructure is separated logically or physically from the production and test infrastructures.

(33) Directly connect [to the agency internal network] – a device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected.

(34) Disaster recovery plan – see Information Technology Disaster Recovery Plan.

(35) Encryption – the reversible process of transforming readable text into unreadable text (cipher text).

(36) Exempt Information – information an agency is not required to disclose under Section 119.07(1), F.S., but which the agency is not necessarily prohibited from disclosing in all circumstances.

(37) Information owner – the manager of the business unit ultimately responsible for the collection, maintenance, and dissemination of a specific collection of information.

(38) Information security – protecting information and information technology resources from unauthorized access, use, disclosure, disruption, modification, or destruction.

(39) Information Security Manager (ISM) – the person designated to administer the agency's information security program in accordance with Section 282.318, F.S.

(40) Information security program – a coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, to assure adequate security for agency information and information technology resources.

(41) Information Technology Disaster Recovery Plan (ITDRP) – information technology resources and procedures to ensure the availability of critical resources needed to support the agency mission in the event of a disaster and to return to normal operations within an accepted timeframe. The ITDRP takes into account availability requirements, recovery time frames, recovery procedures, back-up/mirroring details, systematic and regular testing and training.

(42) Information technology infrastructure – network devices, server hardware, and host operating systems, database management systems, utilities, and other assets required to deliver or support IT services.

(43) Information technology resources – a broad term that describes a set of technology related assets. While in some cases the term includes items such as people and maintenance, as used in this rule, this term means computer hardware, software, networks, devices, connections, applications, and data.

(44) Information technology worker – an agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see User; Worker; Workforce).

(45) Integrity – the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

(46) Interactive session – a work session where there is an exchange of communication between a user and a computer.

(47) Least privilege – the principle that grants the minimum possible privileges to permit a legitimate action in order to enhance protection of data and functionality from faults and malicious behavior.

(48) Malware – malicious software; a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

(49) Management Controls – The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

(50) Media – physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

(51) Mobile computing device – a portable device that can process data (e.g., laptop, personal digital assistant, certain media players and cell phones).

(52) Mobile device – a general term describing both mobile computing and mobile storage devices.

(53) Mobile storage device – portable data storage media including external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), or tape drives that may be easily attached to and detached from computing devices.

(54) National Institute of Standards and Technology (NIST) – a non-regulatory Federal agency within the U.S. Commerce Department's Technology Administration.

(55) Need to know – the principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

(56) Network – an interconnected group of information technology devices; a system that transmits any combination of voice, video and/or data between devices.

(57) Network perimeter – the boundary of an agency's information technology infrastructure.

(58) Operational Controls – security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

(59) Operational information security plan – the agency plan governing the information security program. In addition to detailing the activities, timelines and deliverables for the security objectives that, subject to current resources, the agency will implement during the current fiscal year, the plan includes a progress report for the prior fiscal year, related costs that cannot be funded from current resources, and a summary of agency compensating controls.

(60) Owner – the manager of the business unit ultimately responsible for an information technology resource.

(61) Patch management – the process for identifying, acquiring, testing, installing, and verifying software updates, also known as patches.

(62) Peer to peer – a communications model that allows the direct sharing of files (audio, video, data, and software) among computers.

(63) Personal firewall – software installed on a computer or device which helps protect that system against unauthorized incoming or outgoing network traffic.

(64) Personal information – an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements:

(a) Social Security Number.

(b) Driver's license number or Florida Identification Card number.

(c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Note: as provided in Section 817.5681, F.S., the term personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

(65) Privately-owned device – a device not purchased with agency funds; a device owned by a person or other non-agency entity and not configured, maintained, or tracked by the agency.

(66) Production infrastructure – network devices, server hardware, and host operating systems that comprise an agency's operational or real-time environment.

(67) Public records act – refers to Chapter 119, F.S.

(68) Remote access – any access to an agency's internal network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity). A virtual private network client connection is an example of remote access.

(69) 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.

(70) Risk – the likelihood that a threat will occur and the potential impact of the threat.

(71) Risk analysis – a process that systematically identifies valuable data, information, and information technology 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. (Used interchangeably with risk assessment.)

(72) Risk management – the ongoing process of risk analysis and subsequent decisions and actions to accept risk or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

(73) Security controls – the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed to protect the confidentiality, integrity, and availability of information technology resources.

(74) Security incident – any action or activity, whether accidental or deliberate, that compromises the confidentiality, integrity, or availability of agency data or information technology resources.

(75) Security review – an examination of system records and activities to determine the adequacy of system controls, ensure compliance with established security policy and operational procedures, detect breaches in security, and recommend any indicated changes in any of the foregoing.

(76) Separation of duties – the concept of having more than one person required to complete a task. This is a way to ensure that no one individual has the ability to control all critical stages of a process.

(77) Service account – an account used by a computer process and not by a human (e.g., an account used by the backup process for file access). Normally service accounts may not log on to a system.

(78) Session – the time during which two devices maintain a connection and are usually engaged in transferring data or information.

(79) Smart card – a pocket-sized card with embedded circuits that can process data. Often smart cards are used as a form of authentication for single sign-on systems (also known as integrated circuit card).

(80) Sniffing – capturing network data.

(81) Special trust or position of trust – positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment, pursuant to Section 110.1127, F.S.

(82) Standards – a specific set of practices or procedures to regulate how a system or organization provides services; required practices, controls, components, or configurations established by a recognized authority.

(83) Standard configuration – documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems.

(84) Standard hardware – agency-approved hardware.

(85) Standard software – agency-approved software.

(86) State Chief Information Security Officer – the State of Florida executive responsible for the state government information security posture and direction. This position is appointed by the state Chief Information Officer and oversees the state Office of Information Security.

(87) State Office of Information Security (OIS) – the State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their risks so effective security controls can be implemented. The OIS is part of the Agency for Enterprise Information Technology, pursuant to Section 282.318(3), F.S.

(88) Strategic information security plan – the agency three-year plan that defines security goals, intermediate objectives, and projected agency costs for the strategic issues of information security policy, risk management, security training, security incident response, and survivability.

(89) Strong cryptography – cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Secure Hash Algorithm revision 1 (SHA-1) is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include Advanced Encryption Standard (AES) 128 bits, Triple Data Encryption Standard (TDES), minimum double-length keys, Rivest, Shamir and Adleman (RSA), 1024 bits and higher, Elliptic Curve Cryptography (ECC), 160 bits and higher, and ElGamal (1024 bits and higher).

(90) Survivability – the capability of an organization to maintain or quickly recover critical business functions after a disaster or adverse event, minimize the effect of an event, reduce financial loss, and expedite the return to normalcy.

(91) System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, storing, reporting, printing, dissemination, or disposition of information.

(92) System administrator – a person in charge of managing and maintaining computer or telecommunication systems.

(93) System hardening – the process of securing a system. Hardening typically includes ensuring proper configurations based on intended function, removing non-essential programs and utilities, disabling certain accounts, and installing patches.

(94) System security plan – the plan for an application or information technology resource that describes the security requirements, the controls in place or planned, and roles/responsibilities of all authorized individuals who use the system. A system security plan may also contain critical data policies, backup, disaster recovery, and user policies.

(95) Technical controls – security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

(96) Test infrastructure – a technical environment that mirrors part or all of the production environment and is used for final testing of a technology or an application prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure.

(97) Track – the documented assignment of an asset to a user and/or location.

(98) User – any authorized entity that uses information technology resources (see Worker; Workforce; Information Technology Worker).

(99) Virtual Private Network (VPN) – a communications network tunneled through another communications network.

(100) Warning banner – a message displayed prior to or upon connection to a resource informing the user that activities may be monitored or access is restricted.

(101) Worker – a member of the workforce; a worker may or may not use information technology resources (see User; Workforce; Information Technology Worker).

(102) Workforce – employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the agency, whether or not they are paid by the agency (see User; Worker; Information Technology Worker).

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.003 Agency Information Security Program.

(1) Each agency shall develop, document, implement, and maintain an agency-wide information security program. The goal of the information security program is to ensure administrative, operational and technical controls are sufficient to reduce to an acceptable level risks to the confidentiality, availability, and integrity of agency information and information technology resources.

(2) Each agency head shall appoint an Information Security Manager (ISM) to administer the agency information security program. Within one week of the effective date of appointment, and annually thereafter by January 1, the agency head shall send notification of the Information Security Manager appointment to the State Chief Information Security Officer.

(3) The agency Information Security Manager is responsible for the following duties, which shall also be specified in the agency position description:

(a) Development of a strategic information security plan and associated operational information security plan;

(b) Development and implementation of agency information security policies, procedures, standards, and guidelines;

(c) Development and implementation of the agency information security awareness program;

(d) Coordination of the agency information security risk management process;

(e) Coordination of the agency Computer Security Incident Response Team;

(f) Coordination of Information Technology Disaster Recovery planning in support of the agency Continuity of Operations Plan;

(g) Taking an active role in the agency information technology monitoring and reporting activities;

(4) The agency Information Security Manager shall maintain all agency information security program documents including, the Strategic Information Security Plan, the Operational Information Security Plan, and Security Policies and Procedures.

(5) The agency strategic information security plan must cover a three-year period and define security goals, intermediate objectives, and projected agency costs for the strategic issues of agency information security policy, risk management, security training, security incident response, and survivability.

(6) The agency operational information security plan must include the following items: a progress report for the prior operational information security plan; a project plan that includes activities, timelines, and deliverables for the current fiscal year; related costs that cannot be funded from current resources, and a summary of compensating controls employed by the agency including for each compensating control employed, the implementation date, the target system, and the compensating control description.

(7) The agency Information Security Manager shall review and update the agency Strategic Information Security Plan and the Information Security Operational Plan annually.

(8) By July 31 each year, the agency Information Security Manager shall submit a copy of the agency Strategic Information Security Plan and the Information Security Operational Plan to the State Chief Information Security Officer.

(9) The agency Information Security Manager shall develop, distribute, and periodically update agency information security policies and procedures consistent with this rule.

(10) The agency Information Security Manager, in fulfilling these responsibilities, shall follow the guidelines published by the Agency for Enterprise Information Technology Office of Information Security.

(11) With the approval of the agency head, the agency Information Security Manager may appoint or recommend appointments of individuals from agency offices, divisions, regional agency offices, etc., to be security representatives for their business units. The Information Security Manager shall assign the security responsibilities of the security representatives which shall include serving as security liaison between the unit and the Information Security Manager, promoting security awareness, and ensuring security incident reporting to the Information Security Manager.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.004 Agency Information Technology Workers.

(1) Agency heads are advised to designate information technology positions with access to information processing facilities, or positions that have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate or high as positions of special trust.

(2) Each agency shall conduct background investigations using, at a minimum, Level 2 screening standards and disqualification criteria for personnel in positions of special trust as set forth in Section 110.1127, and Chapter 435, F.S.

(3) Each agency shall provide training for information technology workers to ensure competency in both technical and security aspects of their positions.

(4) Each agency shall establish procedures to ensure administrative rights for information technology resources are restricted to information technology workers who have received appropriate technical training and who are authorized based on job duties and responsibilities.

(5) Information technology workers shall be granted access to agency information technology resources based on the principles of “least privilege” and “need to know.”

(6) Agency Information Security Managers shall give written consent to workers based on job duties and responsibilities before allowing the workers to perform monitoring, sniffing, and related security activities.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.005 Agency Contracts, Providers, and Partners.

(1) Contractors, providers, and partners employed by agencies or acting on behalf of agencies shall comply with this rule, agency security policies, and employ adequate security measures to protect agency information, applications, data, resources, and services.

(2) The agency shall develop procedures to ensure that security requirements are specified throughout the procurement process for information technology services.

(3) Each agency shall ensure contracts and agreements include language whereby the contractor/partner agrees to comply with agency information technology security policies.

(4) Each agency shall ensure that non-agency entities execute a network connection agreement that will ensure compliance with agency security policies prior to allowing non-agency entities to connect to the agency internal network.

(5) Each agency shall maintain a centralized file of network connection agreements.

(6) Each agency shall ensure background investigations using, at a minimum, Level 2 screening standards and disqualification criteria are performed for contractors hired as Information Technology workers with access to information processing facilities, or who have system, database, developer, network, or other administrative capabilities for systems, applications, or servers with risk categorization of moderate or high.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.006 Confidential and Exempt Information.

(1) Agencies shall exercise due diligence to protect exempt, and confidential and exempt information by using appropriate administrative, technical, and physical controls.

(2) Each agency shall maintain a reference list of exempt, and confidential and exempt agency information or software and the associated applicable state and federal statutes and rules.

(3) Each agency shall identify agency information and software that is exempt, or confidential and exempt, under provisions of applicable Florida law or federal law and rules.

(4) Agency information owners are responsible for identifying exempt, and confidential and exempt information.

(5) Exempt, and confidential and exempt information, regardless of format, shall be labeled as such to the extent possible.

(6) Procedures for handling and protecting exempt, and confidential and exempt information shall be referenced in the agency operational information security plan and documented in a policy that is reviewed and acknowledged by all agency staff.

(7) Each agency shall encrypt exempt, and confidential and exempt information sent by e-mail.

(8) Each agency shall encrypt electronic transmission of exempt, and confidential and exempt information when the transport medium is not owned or managed by the agency.

(9) Each agency shall ensure the following:

(a) All passwords are unreadable during transmission and storage using appropriate encryption technology,

(b) Mobile computing devices used with exempt, or confidential and exempt information are encrypted,

(c) Mobile storage devices with exempt, or confidential and exempt agency data have encryption technology enabled such that all content resides encrypted.

(10) For systems containing exempt, or confidential and exempt data, each agency shall ensure written agreements and procedures are in place to ensure proper security for sharing, handling or storing confidential data with entities outside the agency.

(11) Each agency shall destroy exempt, and confidential and exempt information when authorized by the applicable retention schedule, regardless of media type.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.007 Access Control.

(1) Agency information owners shall be responsible for authorizing access to information.

(2) Agency information owners shall review access rights periodically based on risk, access account change activity, and error rate.

(3) Workers shall be authorized access to agency information technology resources based on the principles of “least privilege” and “need to know.”

(4) Each agency shall limit access to information media to authorized workers.

(5) For functions susceptible to fraudulent or other unauthorized activity, the agency shall ensure separation of duties so no individual has the ability to control the entire process.

(6) Access authorization shall be promptly removed when the user’s employment is terminated or access to the information resource is no longer required.

(7) Wireless access into the agency internal network shall require user-authentication.

(8) Only agency-approved wireless devices, services, and technologies may be connected to the agency internal network.

(9) Procedures for granting remote access shall be documented.

(10) Users may remotely connect computing devices to the agency internal network only through agency-approved, secured remote access methods.

(11) Remote access client connections shall not be shared; they are to be used only by the authorized user.

(12) Only agency-owned or agency-managed information technology resources may connect to the agency internal network.

(13) Only agency-owned or agency-managed mobile storage devices are authorized to store agency data.

(14) No privately-owned devices (e.g., MP3 players, thumb drives, printers) shall be connected to agency information technology resources without documented agency authorization.

(15) Mobile computing devices shall be issued to and used only by agency-authorized users.

(16) Mobile computing devices shall require user authentication.

(17) Agency workstations and mobile computing devices shall have enabled a screensaver secured with a complex password and with the automatic activation feature set at no more than 15 minutes.

(18) The agency shall monitor for unauthorized information technology resources connected to the agency internal network.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.008 Awareness and Training.

(1) The agency Information Security Manager shall implement and maintain the agency information security awareness program.

(2) At a minimum, agency workers shall receive annual security awareness training.

(3) Agency workers shall receive initial security awareness training within 30 days of employment start date.

(4) Specialized agency workers (e.g., law enforcement officers) who are required to receive extended off-site training prior to reporting to their permanent duty stations shall receive initial security awareness training within 30 days of the date they report.

(5) Initial training shall include acceptable use restrictions, procedures for handling exempt, and confidential and exempt information, and computer security incident reporting procedures.

(6) The agency shall maintain records of individuals who have completed security awareness training in accordance with the applicable retention schedule.

(7) The agency shall provide specialized training for workers whose duties bring them into contact with exempt, or confidential and exempt information resources.

(8) The security awareness program shall include on-going education and reinforcement of security practices.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.009 Audit and Accountability.

(1) Where possible, audit records will allow actions of users to be uniquely traced to those users so they can be held accountable for their actions.

(2) The agency shall implement procedures to establish accountability for accessing exempt, or confidential and exempt data stores.

(3) The agency shall implement procedures to establish accountability for modifying exempt, or confidential and exempt data.

(4) The agency shall implement procedures to protect the integrity and confidentiality of audit logs.

(5) The agency shall retain audit records as required by the appropriate State, Federal, or other (e.g., Payment Card Industry) schedule.

(6) The agency Information Security Manager, Inspector General, or other specifically authorized personnel shall be granted access to review audit logs containing accountability details.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.010 Certification, Accreditation, and Security Assessments.

(1) The agency shall implement documented procedures to analyze systems and applications to ensure security controls are effective and appropriate.

(2) Information technology resources shall be validated as conforming to agency standard configurations prior to production implementation.

(3) An application security review shall be approved by the application owner, agency Information Security Manager, and Chief Information Officer (or respective documented designee) before a new application or technology is placed into production.

(4) For applications and technologies housed in a primary data center, the application security review shall also be approved by the data center Information Security Manager (or their respective designee) before the new application or technology is placed into production.

(5) An application security review shall be approved by the application owner, agency Information Security Manager, and Chief Information Officer (or designee) before modifications to an application or technology are placed into production.

(6) For applications and technologies housed in a primary data center, the application security review also shall be approved by the data center Information Security Manager (or their respective designee) before modifications to an application or technology are placed into production.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.011 Configuration Management.

(1) The agency shall identify and document information technology resources and associated owners and custodians.

(2) The agency shall specify standard software and hardware.

(3)The agency shall specify and document standard configurations used to harden software and hardware and assure the configurations address known security vulnerabilities.

(4) The agency shall implement a change management process for modifications to production information technology resources.

(5) Agencies shall track agency mobile computing devices.

(6) Mobile computing devices and mobile storage devices shall conform to the following configurations:

(a) Mobile computing devices used with exempt, or confidential and exempt information require encryption.

(b) Mobile storage devices with exempt, or confidential and exempt agency data shall have encryption technology enabled such that all content resides encrypted.

(c) Mobile computing devices connecting to the agency internal network shall use current and up-to-date anti-malware software (where technology permits).

(d) Agency mobile computing devices shall activate an agency-approved personal firewall (where technology permits) when connected to a non-agency internal network.

(e) Only agency-approved software shall be installed on state mobile computing devices.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.012 Contingency Planning.

(1) Data and software essential to the continued operation of critical agency functions shall be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location.

(2) To prevent loss of data, each agency shall develop procedures to ensure agency data, including unique copies of agency data stored on workstations or mobile devices, is backed up.

(3) The agency shall ensure security controls over backup resources are appropriate to the criticality, confidentiality, and cost of the primary resources.

(4) Information technology resources identified as critical to the continuity of governmental operations shall have documented disaster recovery plans to provide for the continuation of critical agency functions in the event of a disaster.

(5) Information Technology Disaster Recovery Plans shall be tested at least annually; results of the annual exercise shall document those plan procedures that were successful and modifications required to correct the plan.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.013 Identification and Authentication.

(1) Agency computer users shall have unique user accounts.

(2) Where technology permits, user accounts shall be authenticated at a minimum by a complex password.

(3) The agency shall ensure accounts with administrative rights are created, maintained, monitored and removed in a manner that protects information technology resources.

(4) The agency shall not use vendor-supplied default passwords.

(5) Administrative account activities shall be traceable to an individual.

(6) The agency shall ensure service accounts are maintained in a manner that protects information technology resources.

(7) Service accounts may be exempted from agency password expiration requirements.

(8) Service accounts shall not be used for interactive sessions.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.014 Incident Response.

(1) Each agency shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to agency management.

(2) The CSIRT membership shall include at a minimum the Information Security Manager, the Chief Information Officer, and a member from the Inspector General’s Office.

(3) The CSIRT shall develop, document, and implement the agency computer security incident reporting process.

(4) The CSIRT shall develop, document, and implement the agency computer security incident response process.

(5) The agency computer security incident response process will include notification procedures to be followed for incidents where investigation determines non-encrypted personal information was, or is reasonably believed to have been, accessed by an unauthorized person, as required by Section 817.5681, F.S.

(6) The CSIRT under the direction of the Chief Information Officer or Information Security Manager shall determine the appropriate response required for each suspected computer security incident.

(7) The agency shall notify the Office of Information Security of computer security incidents including suspected or confirmed breaches within 24 hours of discovery.

(8) Each suspected computer security incident, including findings and corrective actions, shall be documented and maintained as specified in the agency computer security incident procedures.

(9) The CSIRT shall convene at least once a quarter.

(10) The CSIRT shall provide regular reports to the agency Chief Information Officer.

(11) Suspected computer security incidents shall be reported according to agency reporting procedures.

(12) Agency workers shall report loss of mobile devices immediately according to agency reporting procedures.

(13) Agency workers shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency reporting procedures.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.015 Maintenance.

(1) The agency shall ensure information technology resources are correctly maintained to ensure continued confidentiality, availability and integrity.

(2) Agencies shall perform preventative maintenance according to manufacturer specifications for information technology equipment.

(3) Administration of hardware, software, or applications performed over a network shall be encrypted where technology permits.

(4) The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

(5) The agency shall implement service level agreements for non-agency provided technology services to ensure appropriate security controls are established and maintained.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.016 Media Protection.

(1) The agency shall implement procedures to protect agency information from loss, destruction, and unauthorized or improper disclosure or modification.

(2) The agency shall maintain electronic data in accordance with the same retention requirements that apply to agency data in non-electronic formats.

(3) The agency shall sanitize or destroy information media according to the applicable retention schedule and before disposal or release for reuse.

(4) The agency shall document procedures for sanitization of agency-owned computer equipment prior to reassignment or disposal.

(5) Equipment sanitization shall be performed such that there is reasonable assurance that the data may not be easily retrieved and reconstructed. File deletion and media formatting are not acceptable methods of sanitization.

(6) Acceptable methods of sanitization include using software to overwrite data on computer media, degaussing, or physically destroying media.

(7) Users shall take reasonable precautions, based upon applicable facts and circumstances, to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.017 Physical and Environmental Protection.

(1) Information technology resources shall be protected by physical controls.

(2) The agency shall implement procedures to manage physical access to information technology facilities.

(3) Physical controls shall be appropriate for the size and criticality of the information technology resources.

(4) Physical access to central information resource facilities shall be restricted to authorized personnel.

(5) Visitors shall be recorded and, in locations housing systems categorized as moderate impact or high impact, they shall be supervised. (See Rule 71A-1.020, F.A.C.)

(6) Information technology resources shall be protected from environmental hazards (e.g., temperature, humidity, air movement, dust, and faulty power) in accordance with manufacturers' specifications.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.018 System and Application Security Planning.

(1) The agency shall document security controls required to protect the information technology infrastructure.

(2) Application owners shall define application security-related business requirements.

(3) Each agency application or system with a Federal Information Processing Standards (FIPS) 199 categorization of moderate-impact or higher shall have a documented system security plan.

(4) System security plans shall document controls necessary to protect production data in the production infrastructure and copies of production data used in non-production infrastructures.

(5) Production exempt, or confidential and exempt data shall not be used for development.

(6) Production exempt, or confidential and exempt data may be used for testing if: the data owner authorizes the use; test system security controls provide for restricted access and auditing; and production exempt, and confidential and exempt data is removed from the system when testing is completed.

(7) Application security documentation shall be maintained by the agency and be available to the Information Security Manager.

(8) The system security plan is confidential per Section 282.318, F.S. The agency Information Security Manager or designee shall be provided access to system security plans.

(9) Technology managers shall restrict and tightly control the use of utility programs that may be capable of overriding system and application controls.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.019 Personnel Security and Acceptable Use.

(1) Agency workers shall follow agency security policies whenever they are using agency IT resources and data, whether they are inside the agency building or elsewhere.

(2) The agency shall document and implement disciplinary procedures for workers failing to comply with agency security policies and procedures. Disciplinary action shall be appropriate to the violation up to and including termination and/or criminal prosecution as provided by law.

(3) Each agency worker shall agree in writing, to comply with agency acceptable use policies prior to using agency information technology resources.

(4) Agency workers shall agree in writing to comply with agency procedures for handling exempt, and confidential and exempt information prior to accessing exempt, or confidential and exempt information.

(5) Agency workers must obtain documented authorization before taking information technology equipment, software, or information away from the agency facility.

(6) Each agency shall document parameters that govern personal use of agency information technology resources.

(7) The agency shall determine whether an information technology use is personal or business.

(8) Personal use, if allowed by the agency, shall not interfere with the normal performance of a worker’s duties.

(9) Personal use, if allowed by the agency, shall not consume significant amounts of state information technology resources (e.g. bandwidth, storage).

(10) To prevent loss of data, agency users shall ensure unique copies of agency data stored on workstations or mobile devices is backed up.

(11) Agency computer users shall have unique user accounts.

(12) Agency computer users shall be held accountable for activities performed by their accounts.

(13) User accounts shall be authenticated at a minimum by a complex password.

(14) Users shall change their passwords at least every 60 days for high risk systems, every 90 days for moderate risk systems and every 180 days for low risk systems. (See Rule 71A-1.020, F.A.C.)

(15) Agency workers are responsible for safeguarding their passwords and other authentication methods.

(16) Agency workers shall not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

(17) Remote access client accounts shall not be shared.

(18) Agency workers shall immediately report suspected unauthorized account activity according to agency incident reporting procedures.

(19) Agency workers shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency incident reporting procedures.

(20) Agency workers shall have no expectation of privacy with respect to the contents of agency-owned or agency-managed information technology resources.

(21) The agency may inspect all files stored on agency internal network or computer systems, including attached removable media.

(22) The agency may monitor the use of agency information technology resources.

(23) Use of agency information technology resources constitutes consent to monitoring activities whether or not a warning banner is displayed.

(24) Agency computer users shall follow agency-established guidelines for acceptable use of e-mail and other messaging resources.

(25) Exempt, or confidential and exempt information sent by e-mail shall be encrypted.

(26) Inappropriate use of agency e-mail includes the following: distribution of malware, forging headers, propagating “chain” letters, and auto-forwarding agency messages to a private e-mail address.

(27) Agency computer users shall follow agency-established guidelines for acceptable use of Internet resources.

(28) Inappropriate use of the Internet includes unauthorized, non-work related access to the following: chat rooms, political groups, singles clubs or dating services; peer-to-peer file sharing; material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, hate-speech, or violence; hacker web-site/software; and pornography and sites containing obscene materials.

(29) Agency computer users shall log off or lock their workstations prior to leaving the work area.

(30) Workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.

(31) Only agency-approved software shall be installed on agency computers.

(32) Illegal duplication of software is prohibited.

(33) No privately-owned devices (e.g., MP3 players, thumb drives, printers, CDs, DVDs) shall be connected to state-owned information technology resources without documented agency authorization.

(34) Information security activities such as monitoring, sniffing, and related security activities shall be performed only by agency workers based on job duties and responsibilities when given explicit consent.

(35) Agency workers shall not attempt to access information technology resources and information to which they do not have authorization or explicit consent.

(36) Agency information technology resources shall not be used for personal profit, benefit or gain.

(37) Agency information technology resources shall not be used to access, create, store, or transmit offensive, indecent or obscene material unless these activities are a required aspect of the worker’s job duties.

(38) Agency workers shall not use agency information technology resources to engage in activities that may harass, threaten, or abuse others.

(39) Agency information technology resources shall not be used for political campaigning or unauthorized fund raising.

(40) Agency workers shall not circumvent agency computer security measures.

(41) Agency information technology resources shall not be used for any activity which adversely affects the confidentiality, integrity, or availability of information technology resources.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.020 Risk Assessment.

(1) The agency shall categorize information technology resources according to the Federal Information Processing Standards (FIPS) Publication 199, which is hereby incorporated by reference. This process estimates the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource – low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.

		Potential Impact on Agency or State Operations, Assets or Individuals		
		Low Impact	Moderate Impact	High Impact
Security Objective Lost	Confidentiality (unauthorized disclosure)	limited adverse effect	serious adverse effect	severe or catastrophic adverse effect
	Integrity (improper modification or destruction)	limited adverse effect	serious adverse effect	severe or catastrophic adverse effect
	Availability (disruption of accessibility)	limited adverse effect	serious adverse effect	severe or catastrophic adverse effect

(2) The agency shall implement a documented risk management program, including risk analysis for high-impact information resources.

(3) Every three years, the Office of Information Security shall coordinate a comprehensive risk assessment to be conducted in each agency.

(4) The agency Information Security Manager shall submit comprehensive risk assessment findings to the Office of Information Security.

(5) The agency shall implement risk mitigation plans to reduce identified risks to agency information technology resources and data.

(6) The agency Information Security Manager shall monitor and document risk mitigation implementation.

(7) Documentation of an agency's information security risk analysis and risk mitigation plans is confidential pursuant to Section 282.318, F.S., except that such information shall be available to the Auditor General, the Agency for Enterprise Information Technology, and the respective agency's Inspector General.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.021 Systems, Applications and Services Acquisition and Development.

(1) The agency shall perform an impact analysis prior to introducing a new technology. The purpose of this analysis is to assess effects of the new technology on the existing environment.

(2) The agency shall perform an impact analysis prior to modifying current technology, systems, or applications. The purpose of this analysis is to assess effects of the modifications on the existing environment.

(3) The agency shall ensure software applications obtained, purchased, leased, or developed provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, and other information technology resources.

(4) The agency shall develop procedures to ensure that security requirements are specified throughout the procurement process for information technology resources.

(5) The agency shall develop procedures to ensure that security requirements are specified throughout the application procurement process and incorporated into each phase of the application development lifecycle.

(6) The application development team shall implement appropriate security controls to minimize risks to agency information technology resources and meet the security requirements of the application owner.

(7) Agency software applications obtained, purchased, leased, or developed will be based on secure coding guidelines. Some examples of secure coding guidelines are: OWASP [Open Web Application Security Project] Secure Coding Principles – http://www.owasp.org/index.php/Secure_Coding_Principles; CERT Security Coding – http://www.cert.org/secure-coding/, Top 10 Security coding Practices – https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.022 System and Communications Protection.

(1) The Department of Management Services Division of Telecommunications provides the statewide network referred to as SUNCOM. The Department of Management Services establishes standards for SUNCOM network connections and regulates and monitors SUNCOM network connections. (Reference Rules 60FF-1, 60FF-2, 60FF-3, F.A.C.)

(2) Preventative actions taken by agencies to protect information technology resources help ensure the protection of the statewide SUNCOM network and reduce probability of adverse impacts among the agencies that connect to the SUNCOM network.

(3) The agency Information Security Manager or designee shall be granted access to monitor all agency information technology resources.

(4) Technology managers shall monitor technology resources to ensure desired performance and facilitate future capacity-based planning.

(5) The agency shall establish procedures to ensure regular review of system activity logs.

(6) The agency may inspect any files stored on agency internal network or computer systems, including attached removable media.

(7) The agency shall establish and document firewall and router configuration standards that include a current network diagram.

(8) The agency shall ensure network perimeter security measures are in place to prevent unauthorized connections to agency information technology resources.

(9) Databases containing mission critical, exempt, or confidential and exempt data shall be placed in an internal network zone, segregated from the DMZ.

(10) The agency shall monitor for unauthorized network access points.

(11) Unauthorized wireless access points connected to the agency internal network shall be removed immediately upon detection.

(12) Wireless transmission of agency data shall be implemented using strong cryptography for authentication and transmission.

(13) For agency wireless environments, the agency shall change wireless vendor defaults, including default encryption keys, passwords, and SNMP (Simple Network Management Protocol) community strings, and ensure wireless device security settings are enabled for strong cryptography technology for authentication and transmission.

(14) Agencies shall establish procedures to ensure agency cryptographic implementations are developed and maintained according to the Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules (2001).

(15) Key management processes and procedures for cryptographic keys used for encryption of data will be fully documented and will cover key generation, distribution, storage, periodic changes, compromised key processes, and prevention of unauthorized substitution.

(16) Key management processes must be in place and verified prior to encrypting data at rest (including e-mail messages, data files, hard drives, data backups).

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.

71A-1.023 System and Information Integrity.

(1) Controls shall be established to ensure the accuracy and completeness of data.

(2) The development and test infrastructures shall be physically or logically separated from the production infrastructure.

(3) A sufficiently complete history of transactions shall be maintained for each session involving access to critical information to permit an audit of the system by tracing the activities of individuals through the system.

(4) Individuals accessing critical information shall be uniquely identified.

(5) The agency shall ensure anti-malware software is maintained on agency information technology resources.

(6) The agency shall implement a patch management process for information technology resources.

(7) The Agency for Enterprise Information Technology Office of Information Security will monitor the Internet and appropriate global information security resources for any abnormalities or threats present on the Internet and provide relevant Security Alerts to state agencies.

(8) Application developers shall incorporate validation checks into applications to detect data corruption that may occur through processing errors or deliberate actions.

Rulemaking Authority 14.204(7), 282.318(3), 282.318(6) FS. Law Implemented s. 12, Ch. 2009-80, L.O.F. History–New 11-15-10.