POLICY SERIES:	Information Security
POLICY TITLE:	Acceptable Use (This is to replace the current policy titled "Employee Responsibilities Regarding Information Technology Resources and Databases".)
POLICY NUMBER:	2.8 (Current Number)
EFFECTIVE DATE:	Unknown
REVISION DATE:	05/01/2013 (03/05/2013) (10/16/2012) (1/26/2010)
PAGE(S):	21

1.0 Policy Statement:

Members of the DOE workforce are responsible for compliance with state, federal, and local laws and the Department's policies regarding information technology use and resource security. Technologies provided by the Department to members of the DOE workforce are for official business use to enable users to carry out the goals, objectives, and mandates of the Department.

This policy serves as notice that the Department reserves the right to track user Internet, email, computer accesses, and telephone usage. DOE monitors DOE network, server, and workstation activity; therefore members of the DOE workforce must understand that use of DOE information technology resources is subject to being actively monitored.

In accordance with Section 282.318, Florida Statutes, all Department of Education workers are required to read and sign the form found in section 7.0 Applicable Forms, at the end of this policy. The signed statement shall be placed in the worker's official personnel file.

Any violations of the policies contained herein are grounds for disciplinary action up to and including dismissal.

2.0 Policy Scope:

This policy applies to all Department of Education employees, contractors, consultants, temporary employees, and other workers including all personnel affiliated with third parties utilizing DOE information technology resources.

3.0 Definitions:

3.1 Ad-hoc network - A term used to describe a device-to-device network; an informal way of creating a wireless network between two or more computers without the need for a centralized access point

3.2 Agency network - A collection of devices and networks interconnected so that the aggregate collection operates as a single network entity which is isolated via one or more perimeter devices (i.e., firewalls, routers) from other networks which do not belong to, or are not a part of the agency network. Isolated demilitarized zones (DMZs) or interagency red zones normally are not considered part of the agency network; however, DMZs for which connectivity to non-agency networks is run through the agency network, or that have connectivity to the agency network are considered part of the agency network. Connectivity to the agency network is not intended for guest wireless services.

3.3 Anti-malware software - Software installed on a computing device that protects it from malicious software.

3.4 Anti-spyware - Program designed to remove or block spyware (computer software that collects personal information about users without their informed consent).

3.5 Anti-virus software - Computer programs that attempt to identify, thwart, and eliminate computer viruses and other malicious software (malware).

3.6 Authentication - The process of verifying that a user, process, or device is who or what it purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint, voice pattern, or retinal scan.

3.7 Authorization - Official or legal permission or approval.

3.8 Availability - The principle that authorized users have access to information and assets when required.

3.9 BIOS (Basic Integrated Operating System) - Refers to the software code run by a computer when first powered on. The primary function of the BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer.

3.10 Blogging - A Web site that contains an online personal journal with reflections, comments, and often hyperlinks provided by the writer.

3.11 Breach – Unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.

3.12 Cable lock - A physical security device connecting the mobile device to an immovable object to deter theft.

3.13 Chief Information Officer - The person who coordinates all information resource management activities and information technology assets to ensure they are appropriately planned and managed in accordance with the agency mission.

3.14 Cloud Computing - Cloud computing in its simplest form, refers to information technology services, accessed via the Internet, where the location of the infrastructure is unknown to the user. Some examples of cloud services are Microsoft Hotmail, Gmail, Facebook, Dropbox, and YouTube, although there are many more. Most of these popular cloud services are free.

3.15 Confidentiality - The principle that information is accessible only to those authorized to have access.

3.16 Configuration - Documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems.

3.17 DOE internal network - See definition for agency network.

3.18 DOE Personnel Management - The DOE Bureau of Personnel Management, formally known as the Personnel Office.

3.19 ECM Agent (Enterprise Configuration Manager) - An agent that runs on DOE workstations to collect system data, not user data.

3.20 Email header - In an email, the text (body) is preceded by header lines indicating sender, recipient, subject, sending time stamp, receiving time stamp of all intermediate and the final mail transfer agents, and much more.

3.21 Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.

3.22 Extranet - An intranet that is partially accessible to authorized persons outside of a company or organization.

3.23 Family Educational Rights and Privacy Act (FERPA) - Federal standards protecting the privacy of education records.

3.24 Guest Wireless – A separate network intended for wireless internet connectivity by DOE users and guests. Users of this network are not able to connect to the DOE internal network.

3.25 Hardware - The mechanical, magnetic, electronic, and electrical devices comprising a computer system, such as the CPU, disk drives, keyboard, or screen.

3.26 Host-based IDS (Intrusion Detection System) - A special category of an Intrusion-Detection System (detects unwanted manipulations to computer systems, mainly through the Internet) that focuses its monitoring and analysis on the internal interfaces of a computing system rather than on its external interfaces.

3.27 Inappropriate material - Defined as text, photographic images, graphic representations or video materials that include but are not necessarily limited to: profane, scandalous, pornographic, suggestive or explicit sexual content; harassing messages; abusive, offensive, vulgar, obscene, or otherwise unprofessional content; or content related to chain letters, gambling, wagering, betting or other activity related to a game of chance, trial, contest, or sporting event.

3.28 Information Security Manager (ISM) - The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318, Florida Statutes, and the agency's internal and external point of contact for information security matters.

3.29 Information Technology Resources - Agency computer hardware, software, networks, devices, connections, applications, and data. This can also include video equipment, audio equipment, telephones, fax machines, copiers, cell phones, pagers, and other technology-oriented devices.

3.30 Information Technology Worker – an agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see definitions for User, Worker, and Workforce).

3.31 Integrity - The principle that assures information remains intact, correct, and authentic. Protecting the integrity involves preventing unauthorized creation, modification, or destruction of information.

3.32 Internal network - See definition for agency network.

3.33 Internet - A vast computer network linking smaller computer networks worldwide.

3.34 Intranet - A computer network with restricted access, as within a company, that uses software and protocols developed for the Internet.

3.35 Local Area Network (LAN) - A system for linking a number of microcomputers, terminals, work stations, etc., with each other or with a mainframe computer in order to share data, printers, information, programs, disks, etc.; usually confined to one office, building, or agency.

3.36 Malware - Software, such as viruses, worms, or Trojan horses intended to damage or disable a computer system. It can also include spyware that covertly obtains information from a computer. The term is short for malicious software.

3.37 Media - A storage vessel for electronic data and information (e.g., hard drive, laptop, CD, tape, thumb drive).

3.38 Microblogging - Blogging done with severe space or size constraints typically by posting frequent brief messages about personal activities.

3.39 Mobile Computing Device - A laptop, smart phone, or other portable device that can process data.

3.40 Mobile Devices - A general term describing both mobile computing and mobile storage devices.

3.41 Mobile Storage Device - Portable data storage media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), iPods, media players, cell phones, or tape drives that may be easily attached to and detached from computing devices.

3.42 Modem - An electronic device that makes possible the transmission of data to or from a computer via telephone or other communication lines.

3.43 Need-to-Know – The principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

3.44 Network - A system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables used to transmit or receive information.

3.45 Network Interface Card (NIC) - An adapter circuit board installed in a computer to provide a physical connection to a network.

3.46 Online storage – see Cloud Computing.

3.47 Password - A form of secret authentication data that is used to control access to a resource.

3.48 Personal firewall - Software installed on a computer or device which helps protect that system against unauthorized access.

3.49 Port scanning - When a software tool is used to search a network host for open ports. This is often used by administrators to check the security of their networks and by malicious users to compromise it.

3.50 Public information - All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency which is not confidential and has not been exempted from public disclosure by statute.

3.51 Public records - All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. Section 119.011(12), F.S.

3.52 Real-time scanning - A feature of many anti-malware programs which monitor computer systems for suspicious activity such as viruses, spyware, adware, and other malicious objects in 'real-time' i.e., while surfing the web or running an application.

3.53 Short Message Service (SMS) - SMS stands for short message service. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

3.54 Signature file - Pattern file used by anti-malware programs to identify existing malware. Out-of-date signature files will allow newer malware threats to go unnoticed.

3.55 SMS - See definition for Short Message Service.

3.56 Sniffing - Capturing network data.

3.57 Social media - Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).

3.58 Standards - A specific set of practices or procedures to regulate how a system or organization provides services.

3.59 Text messaging - Sending short text messages to a device such as a cellular phone, PDA or pager. Text messaging is used for messages that are no longer than a few hundred characters. The term is usually applied to messaging that takes place between two or more mobile devices.

3.60 Transitory - Transitory messages are those intended to communicate information of short-term value. Examples of transitory messages include: reminders about scheduled meetings or appointments; most telephone messages; notifications

such as “I will be 10 minutes late,” etc. “Transitory” refers to short-term value based upon the content and purpose of the message, not the format or technology used to transmit it. Transitory messages are not intended to formalize or perpetuate knowledge.

3.61 Trojan horse - A malicious program that is disguised as or embedded within legitimate software.

3.62 User - Any authorized entity that uses information technology resources (see definitions for Worker, Workforce, and Information Technology Worker).

3.63 Virus - A parasitic software program, equipped with the means of reproducing itself, which spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of itself.

3.64 Wireless Access Point (WAP or AP) - A device that connects wireless communication devices together to form a wireless network. The WAP usually connects to a wired network, and can relay data between wireless devices and wired devices.

3.65 Wireless network - A computing network made up of, but not limited to, computers and access points or repeaters joined by radio communication using a frequency spread-spectrum technology.

3.66 Worker – A member of the workforce, a worker may or may not use information technology resources (see definitions for User, Workforce, and Information Technology Worker).

3.67 Workforce - Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct or contractual control of the department, whether or not they are paid by the agency (see definitions for User, Worker, and Information Technology Worker).

3.68 Workstation - A computer used by members of the workforce for work-related duties.

3.69 Worm - A self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer

4.0 Guidelines:

Questions regarding this policy should be directed to the Department of Education Information Security Manager (ISM).

DOE Policies referenced in this document should be reviewed and understood if applicable to the user. Additional reference policies are as follows:

- Computer Security Incident Response
- Data Classification and Handling
- DOE Wireless (Wi-Fi) Acceptable Use

- Mobile Devices
- Personal Hand-Held Mobile Computing Devices
- Remote User Access

5.0 Procedures:

5.1 Compliance with Applicable Laws

5.1.1 It is the responsibility of the user having access to the information technology resources and databases of the Department of Education (DOE) and the State of Florida (State) to read and understand the Department's policies and procedures regarding the acquisition of resources, disposal of resources, the security of data and resources (see the Department's Code of Personal Responsibility). All members of the DOE workforce are to abide by all of the policies and procedures. The willful and knowing unauthorized use, alteration, or destruction of information technology resources and databases is a computer-related crime punishable under Chapter 815, Florida Statutes.

5.1.2 Each member of the DOE workforce is responsible for complying with applicable State and Federal security rules and laws, and with the agency's security policies and procedures when performing agency work or when using agency information technology resources.

5.2 Computer Use and Confidentiality Agreement

5.2.1 Each member of the DOE workforce is to acknowledge, in writing, these responsibilities by completing an agency acceptable use and confidentiality agreement prior to the use of DOE information technology resources. The agreement form is in Section 7.0 of this document. The completed form must be turned in to the appropriate personnel liaison for inclusion in the employee's official personnel file.

5.3 Use of DOE Information Technology Resources

5.3.1 Access to agency information technology resources is reserved for agency authorized users.

5.3.2 Workers must not use computer equipment that is not assigned to them without prior supervisory approval.

5.4 Personal Use of Information Technology Resources

5.4.1 It is recognized that, from time to time, occasions may arise wherein the limited use of information technology resources for a personal reason may be permitted and in the best interest of the Department and its users.

5.4.2 Personal use of technologies may be approved by supervisors as appropriate and within the following guidelines:

a. The use of information technology resources for personal requirements shall not interfere with the users or any co-worker's job responsibilities or assigned tasks.

b. The usage shall occur on a user's own time, e.g., during a break or lunch period, except as otherwise authorized.

c. All such usage shall be kept to a minimum and not incur any measurable cost to the state, in use of paper, ink or wear and tear on the equipment.
Note: Personal usage may result in reimbursement for costs associated with personal use.

5.4.3 Workers are responsible for complying with state, federal, and local laws and the Department's policies on technology use and resource security.

5.5 Access Authorization and Authentication

5.5.1 Agency computer users shall have unique user accounts.

5.5.2 Agency computer users shall be held accountable for their account activities.

5.5.3 User accounts shall be authenticated at a minimum by a user ID and password.

5.5.4 Agency computer users are responsible for safeguarding their passwords and other authentication methods.

5.5.5 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.

5.5.6 Agency workers shall immediately report suspected account compromises to their supervisor and to the DOE Information Security Manager.

5.5.7 Agency workers shall immediately report lost security tokens, identification badges, or other devices used for identification and authentication purposes according to agency incident reporting procedures.
(See the Computer Security Incident Response Policy for additional information.)

5.5.8 Supervisors shall:
- Approve the assignment of employee or user IDs for access to data;
- Initiate access to other specialized applications;
- Provide the Education Data Center with written requests to delete all IDs of terminated employees or other workforce members.

5.5.9 Supervisors shall also be responsible for ensuring that the Education Data Center and specialized application managers are notified when employees or other workforce members terminate from the Department by notifying the Personnel Office in an email.

5.5.10 DOE Personnel Management shall notify the DOE Helpdesk of all workforce terminations. The appropriate Education Data Center staff

shall immediately disable all applicable IT resource user IDs and accesses. The Data Center staff shall notify the DOE ISM of the action taken upon completion.

5.6 User Privacy

5.6.1 The agency shall be allowed to inspect any and all files stored on agency network or computer systems, including attached removable media.

5.6.2 DOE shall be allowed to monitor the use of its information technology resources.

5.6.3 Use of DOE information technology resources constitutes consent to monitoring activities whether or not a warning banner is displayed.

5.7 Public Records / Information

5.7.1 Any information generated through a computer, stored on disk, or electronically mailed is subject to all rules governing public records. (Public Records, Chapter 119, F.S.).

5.7.2 With few exceptions, information generated through a Department computer, stored on any media, or sent or received electronically, such as email, is a public record. These records are subject to all laws governing the maintenance and disposal of public records. For further information, consult the Department's Public Records Policy.

5.8 Access to Information and Data

5.8.1 Users working with confidential information must follow the standards outlined in the Data Classification and Handling Policy.

5.8.2 Except as provided below, users must view only technology information or data they are authorized to view to do their job. (See definition for Need-to-know.)

5.8.3 Users who become aware of a suspected or actual information security breach must contact the DOE Helpdesk and/or the Information Security Manager.

Personally Identifiable Student Records

5.8.4 Users who have access to personally-identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Section 1002.22 F.S., and Section 1008.39 F.S., and other applicable laws and regulations, as they relate to the release of student information.

5.8.5 Users shall not use access to student records information for personal gain. In no case shall personally-identifiable information be released publicly.

5.8.6 Users are to refrain from viewing or printing personally-identifiable information except to perform their assigned duties.

5.8.7 Users authorized to access personally-identifiable information shall execute a separate acknowledgment indicating they are aware of additional provisions of applicable laws and regulations. The form shall be

provided by and kept on file by the business unit that owns or oversees the information.

People First Employee Data

5.8.8 The People First System enables employees to record time, attendance, leave, and personal information. Employees who use or have access to this information must use such information for a legitimate business purpose only. Employees are prohibited from disclosing confidential information accessed in the system or from using the information for personal purposes or personal gain.

5.8.9 The "casual viewing" of employee data constitutes misuse of access, is not acceptable, and will not be tolerated. Database queries are performed by People First and the Department of Management Services on a regular basis to identify misuse of the People First System. Violators of this policy will be subject to disciplinary action, up to and including dismissal, and may be subject to criminal prosecution.

5.9 System and Network Activities

5.9.1 Only authorized IT staff are to connect network devices and/or microcomputers to the existing DOE network.

5.9.2 Users shall not connect any device to the DOE internal network without the knowledge and written authorization of the Data Center Director and the Information Security Manager.
Note: This does not include the DOE wireless guest network. The DOE guest wireless network will allow any wireless device to connect to the internet.

5.9.3 Only authorized users may create and publish websites.
For further information contact the DOE Communications Office.

5.10 Copyright

5.10.1 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which there is no active license is strictly prohibited.

5.10.2 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Department's General Counsel shall be consulted prior to export of any material that is in question.

5.11 Prohibited Uses

5.11.1 Users shall not introduce malicious programs or tools into the network or server environment (e.g., viruses, worms, Trojan horses, email bombs, etc.).

5.11.2 Using any computing asset to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is prohibited.

5.11.3 Making fraudulent offers of products, items, or services originating from any State of Florida account is prohibited.

5.11.4 Users shall not engage in port scanning activities of any kind unless preapproved in writing by the DOE Information Security Manager and Chief Information Officer.

5.11.5 Users shall not circumvent user authentication or security of any host, network, or account.

5.11.6 Users shall not participate in disruptions of network communication, unless this activity is scheduled and is a part of the user's normal job/duty, which includes but is not limited to:

a. Introducing any process resulting in a cyber attack or denial of service attack.

b. Executing any form of network monitoring/sniffing that consumes or absorbs bandwidth or increases traffic.

c. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's computing session, via any means, locally or via the Internet/Intranet/Extranet.

5.11.7 Effecting security breaches which include but are not limited to, accessing data to which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access is prohibited, unless these duties are within the scope of regular duties.

5.11.8 Agency computer users shall not attempt to access information technology resources for which they do not have authorization or explicit consent.

5.11.9 Users shall not provide access to confidential or proprietary information to unauthorized individuals.

5.11.10 DOE information technology resources shall not be used for any purpose which violates state or federal laws or rules.

5.11.11 DOE information technology resources shall not be used for personal profit, benefit or gain, or to promote or benefit an individual or private business.

5.11.12 DOE information technology resources shall not be used to access, create, store, or transmit offensive, indecent, or obscene material.

5.11.13 Agency computer users shall not use DOE information technology resources to engage in activities that may harass, threaten, or abuse others.

5.11.14 DOE information technology resources shall not be used for political campaigning or unauthorized fund raising.

5.11.15 Agency computer users shall not circumvent agency computer security measures.

5.11.16 DOE information technology resources shall not be used for any activity that adversely affects the availability, confidentiality, or integrity of information technology resources.

5.12 Electronic Data Communications

Transmitting by email, instant message, chat, or any other electronic means, or viewing on the Internet any inappropriate material is strictly prohibited. (See definition for Inappropriate material.)

Email

Messages sent as electronic mail (email) shall meet the quality standards for distribution and display as if they were tangible documents or instruments. When sending messages, users shall abide by all security restrictions on information to which they have access, regardless of whether the email is accessed from within the Department or through remote access. Electronic mail shall be used for Department-related purposes and not for personal use or gain.

5.12.1 Agency computer users shall follow agency established guidelines for acceptable use of email resources.

5.12.2 Email containing confidential information must be encrypted or transmitted via an approved DOE solution. (Contact the DOE ISM for information regarding secure email.)

5.12.3 Inappropriate use of agency email includes, but is not limited to, the following:

a. distribution of malware;
b. forging email headers;
c. propagating “chain” letters; and
d. auto-forwarding agency email to a non-agency email address.

5.12.4 If a user receives an email containing inappropriate material, the user must take the following action:

a. If the sender of the email is personally known to the user, the user must:
   - Refrain from replying, forwarding, or deleting the email;
   - Notify the sender by phone or in a separate email to cease sending such materials since receipt or transmission of such material is inconsistent with Department policy; and
   - Inform his or her supervisor of receipt of the inappropriate email.

b. If the sender of an inappropriate email is not known by the user, the user must:
   - Refrain from replying, forwarding, or deleting the email;
   - Inform his or her supervisor immediately that an inappropriate email has been received; and

- Follow the supervisor's instructions on the deletion or removal of the offensive information.

Internet

Internet access and associated resources shall be used by workers to assist and enhance job productivity as it relates to Department business. These resources shall be used for Department-related purposes and not in any manner that will not result in direct or indirect benefits to the Florida Department of Education. (For exception see section 5.4 – Personal Use of Information Technology Resources.)

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

5.12.6 The Internet is not to be used to conduct any activities, which would be illegal under federal, state, or local laws, or would be otherwise prohibited under rules in the Florida Administrative Code.

5.12.7 Inappropriate use of the Internet includes non-work related access to the following:

a. chat rooms, political groups, singles clubs, or dating services;
b. material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, or violence;
c. hacker websites/software; and
d. pornography.

Instant Messaging / Chat

5.12.8 Only authorized DOE Instant Messaging that archives messages for public records is allowed to be used on systems connected to the DOE network.

5.12.9 Chat is not permitted on the DOE network.

Use of Personal Text Messaging

5.12.10 Each and every department employee is prohibited from conducting agency business via personal text messaging or other means of written communications that are not archived by DOE for public records. This would include but not be limited to short message service (SMS), instant messaging, cell phone texting, other similar technology, social media (i.e., Facebook, Twitter, etc.), or personal e-mail. See definitions for text messaging, SMS, and social media.

5.12.11 If a Department employee receives a message related to agency business via personal text messaging, the employee should immediately inform the sender of this policy, and demand that future communications be sent via approved methods (i.e., the employee's fldoe.org email address or telephone).

5.12.12 The employee shall also forward the improper communication to their fldoe.org email address to ensure that the record is properly retained.

5.12.13 Any known or suspected violation[[~~s~~]] of this policy should immediately be reported to management for investigation. Violations may result in discipline up to and including dismissal.

5.12.14 The Department understands that there may arise the occasion where employees may need to communicate with each other via personal text messaging. Such communication is permissible under this policy provided that the message is transitory in nature. See definition for transitory.

5.12.15 There is no prohibition against Department employees communicating via text messaging, social media, or personal e-mail provided that the communication is in no way related to agency business.

5.13 Non-DOE Computers

5.13.1 Computers not issued by DOE are not permitted to directly connect to the internal DOE internal network. See section 5.30 for exceptions.

5.14 Software

5.14.1 All software on computers must be licensed. Workers are responsible for using software in accordance with licensing agreements. Users must observe copyright restrictions held by the Department or State. Workers who use or have access to software are responsible for knowing and complying with all applicable terms and conditions regarding its use.

5.14.2 Users must not make or distribute unauthorized copies of software. Modifications cannot be made to the software that are not authorized by the copyright holder. A copyright legend or notice shall not be removed from the software or any of its documentation.

5.14.3 Commercial microcomputer software purchased by DOE is authorized for DOE use only. Making copies of DOE-purchased software for personal use is illegal and prohibited.

5.14.4 Users must contact the Education Data Center when questions arise as to terms, conditions, and restrictions on information technology resources and databases.

5.14.5 Even though an employee has terminated their employment with the Department, the former employee can be personally subject to legal action by infringing upon copyright or intellectual property rights.

5.14.6 Beta software is not supported, nor can it be installed on production computers without written approval from the Data Center Director. If there is a need to test beta software for a project, the testing shall be done in a DOE-approved test environment.

5.14.7 Applications known to promote adware are not allowed on the desktop.

5.14.8 Users shall not install personally owned software on DOE-owned information technology resources. See Section 5.30 for exceptions.

5.14.9 Only software with valid licensing shall be installed on DOE-owned information technology resources.

5.14.10 Users shall not install any program files (executable, shareware, freeware), or personal files on their network home directory or on any network drive.

5.14.11 Users shall not install software on their assigned computing device. Authorized IT staff are to install software necessary to perform job duties.

5.14.12 No software that promotes or enables peer-to-peer file sharing functionality will be allowed on any computer connected to the DOE network.

5.15 Hardware

5.15.1 Hardware and related equipment acquired by the State or Department shall be used exclusively for Department business.

5.15.2 Users shall not use any DOE-issued hardware or related equipment for private business or personal use. (For exceptions, see section 5.4 – Personal Use of Information Technology Resources.)

5.15.3 Users shall not use DOE-issued hardware to access information not related to their assigned responsibilities, and it shall not be used for recreational purposes such as computer games, accessing Internet sites that are not work related, or for production of printed materials for other than Department business. (For exceptions, see section 5.4 – Personal Use of Information Technology Resources.)

5.15.4 Transfer of IT hardware requires the user to complete a Property Transfer Form. For additional information contact the DOE's Bureau of General Services or the appropriate Property Custodian.

5.16 User Data

5.16.1 Only user data saved in the user's network directories on the LAN (Local Area Network) file servers will be backed up by DOE IT staff. The user's network home directory is for the storage of data files that are created by application programs on the user's desktop computer.

5.16.2 Users are responsible for ensuring their data is stored on network drives or to ensure their data is backed up in a manner that the data can be recovered in the case of theft, loss, or system crash.

5.16.3 Users shall not use free online (Cloud Computing) storage solutions to store DOE data. Only entities that are under contractual agreement with DOE shall be used to store DOE data and information. See section 5.30 for exceptions.

5.17 Wireless

5.17.1 No end-user at any time is authorized to setup a wireless access point on DOE premises. The installation of wireless connectivity is to be under the control of DOE IT staff with the knowledge and approval of the CIO and ISM. To ensure security, all unauthorized wireless access points will be shut down immediately upon discovery.

5.17.2 Users shall not run their laptops in wireless ad-hoc mode. This potentially allows other users to connect to the laptop in a peer-to-peer connection.

5.17.3 DOE supports public and private wireless connectivity. Users wishing to utilize DOE wireless access must follow the standards outlined in the DOE Wireless (Wi-Fi) Acceptable Use Policy.

5.18 Network

5.18.1 Monitoring, sniffing, and related security activities shall be performed only by workers based on job duties and responsibilities when given explicit consent.

5.19 Desktop Security

5.19.1 Users shall NOT remove and/or in any way attempt to disable any IT security software installed and/or configured by the DOE IT staff. This can include, but is not limited to, the following: anti-virus software, anti-spyware software, password enabled screen-saver utility, personal firewall, ECM agent, and/or host-based IDS.

5.20 Anti-Virus / Anti-Spyware

5.20.1 Any PC-based computer or laptop that connects to the DOE internal network shall have anti-virus and anti-spyware software installed and scheduled to run complete scans at regular intervals.

5.20.2 Any PC-based computer or laptop that connects to the DOE internal network shall have anti-virus and anti-spyware software installed and running in the background to perform real-time scanning while the system is in use.

5.20.3 The anti-virus and anti-spyware software and signature files shall be kept up-to-date.

5.20.4 Unauthorized personnel shall not modify the configuration of DOE provided anti-virus and anti-spyware protection software after installation.

5.21 Computer Lockdown

5.21.1 Users shall lock their workstation, or log out, whenever their workstation is unattended.

5.21.2 Screen savers on all operating system platforms (Windows XP, etc.) shall have passwords set to engage after 15 minutes or less of inactivity.

5.21.3 Authorization for applying a power on password (BIOS enabled passwords) shall come from the Data Center Director.

5.22 Dual Connectivity

5.22.1 Desktop computers are not permitted to have both a network interface card (NIC) and modem. This creates a potential security violation.

5.22.2 Laptops are NOT included in this standard. However, while laptops may have a NIC, with wireless and modem capabilities, they are not to be connected simultaneously. That is, a user is not to dial-in to an Internet service provider and at the same time be connected to the DOE LAN.

5.22.3 Users shall not set up their computer or laptop to accept dial-in connectivity.

5.23 Laptops

5.23.1 Security mechanisms to protect both the physical asset (laptop) and the information contained by the laptop (data) are to be implemented and maintained.

5.23.2 New laptop purchases are to be purchased with approved security cable locks. Cable locks are to be purchased and put in use for all existing DOE laptops.

5.23.3 Laptops used as workstations shall be secured with a cable lock or with a locked-down docking station.

5.23.4 Laptops used remotely must follow the standards outlined in the Remote User Access Policy.

5.23.5 All confidential or sensitive data stored on a DOE laptop shall be encrypted with an approved encryption solution. Contact the DOE ISM for further information.

5.23.6 The laptop user is responsible to ensure all data stored on a DOE laptop is backed up in a manner that the data can be recovered in the case of theft or system crash.

5.23.7 In the event that a laptop is lost or stolen, the user is to follow appropriate DOE procedures. (See section 5.26 – Stolen or Missing Equipment.)

5.24 Mobile Devices

5.24.1 Users who wish to use their personal mobile devices for email and calendaring synchronization with DOE resources must follow the standards outlined in the **Personal Hand-Held Mobile Computing Devices Policy** of Information Security Management.

5.24.2 Users with DOE-issued mobile devices must follow the standards outlined in the Mobile Devices Policy.

5.25 Remote Management

5.25.1 Users are not to remove or disable the remote management client from their desktop. If problems seem to be related to the remote management client, then the DOE IT staff, at their discretion, will disable the client or modify the configuration.

5.25.2 Remote management of a user's computer shall require the user's knowledge and explicit permission. This requirement will be waived in the event of a formal investigation with the written permission of the CIO or the Inspector General.

5.26 Maintenance

5.26.1 Workstations and laptops shall be maintained with the latest software patches, anti-virus and anti-spyware signatures, updates, and software rollouts. In order to facilitate this process, users shall observe the

procedures outlined by their respective data center regarding information technology resource maintenance schedules.

5.27 Stolen or Missing Equipment

5.27.1 Users are responsible for securing State property. Users who believe their State or personal property has been stolen should immediately report the suspected theft to the Office of the Inspector General at (850) 245-0403. The suspected theft also should be reported to the users' immediate supervisor and to the appropriate Property Custodian.

5.27.2 The DOE Information Security Manager must be notified in the event of any suspected or actual loss or theft of a laptop, or any media (see definition for Media) that contained DOE information or data.

5.28 Security Awareness Training

5.28.1 Users must annually participate in information security awareness training. Training is provided by the Information Security Manager and can be taken in a variety of formats. Lunch-n-learn, PowerPoint, scheduled sessions with the ISM, and/or online via the information security webpage on the DOE intranet.

5.28.2 All new hires and new contractors are to participate in the new hire orientation that includes an Information Security Awareness module.

5.29 Enforcement

5.29.1 Violation of these standards may result in the agency taking disciplinary action appropriate to the violation, up to and including termination and/or criminal prosecution.

5.30 Exceptions

Use of Non-DOE Computers

5.30.1 The use of non-DOE computers and associated equipment in support of State-related work at the home or the work place is discouraged; however, it may be authorized if properly certified. (Forms may be obtained from the DOE Helpdesk or the Information Security Manager.)

5.30.2 DOE is not responsible for non-DOE computers damaged or needing repair as the result of State-related work.

5.30.3 Users shall certify that their non-DOE computer meets or exceeds the DOE security standards outlined below.

a. The operating system shall have the latest patches applied. Any operating system no longer supported is not permitted to connect directly to the DOE network. (For further information contact the DOE ISM.) For example, this would include Windows 97. Windows XP will be retired in April of 2014.
b. Windows systems shall be running an up-to-date anti-virus and anti-spyware solution with up-to-date signature files.
c. Windows, Macintosh, and Linux systems shall run a personal firewall.

d. Windows, Macintosh, and Linux systems shall run a password enabled screen saver.
e. Windows, Macintosh, and Linux systems shall keep security patches and updates current.

5.30.4 Computers not issued by DOE shall not be allowed to connect directly to the DOE internal network without approval. (Forms may be obtained from the DOE Helpdesk or the Information Security Manager.)

5.30.5 Use of a non-DOE computer must be approved by the Information Security Manager and the record of approval shall be maintained by the Information Security Manager.

5.30.6 At a minimum, approval for non-DOE computers shall be renewed annually.

5.30.7 The computer owner is responsible for meeting all established DOE standards for copyrighted software.

5.30.8 The individual owner is responsible for the maintenance and repair of non-DOE computers.

Use of Free Cloud Computing Solutions for File Transfers

5.30.9 Use of cloud computing solutions (e.g., Dropbox, box, YouSendIt, SkyDrive, etc.) cannot be used at any time for restricted or confidential data or information. There are no exceptions to this standard.

5.30.10 Use of cloud computing solutions for the transfer of public DOE data that cannot be accommodated by DOE's email solution must be approved in writing by the DOE ISM. A Helpdesk request must be initiated by the requestor for assistance with this need.

Use of Personally Owned Software

5.30.11 Personal software must be properly licensed and the software owner must be able to demonstrate legitimate ownership.

5.30.12 Personal software must be for work purposes, not for desktop enhancements (e.g., screen saver applications, photo organizers, etc.)

5.30.13 Use of personal software must be approved by Desktop Support and the ISM.

6.0 Reference Documents:

Chapter 119, Florida Statutes

Section 282.318, Florida Statutes

Chapter 815, Florida Statutes

Section 1002.22, Florida Statutes

Section 1008.39, Florida Statutes

Chapter 71A-1, Florida Administrative Code

Family Educational Rights and Privacy Act (FERPA)

7.0 Applicable Forms:

Appendix A: Acknowledgement of Compliance with Information Security Policies - The signed form is to be kept on file with the DOE Personnel Office.

8.0 Department Contact:

Division/Section/Office Name:	Office of Technology and Information Services
Suite number:	1144 Turlington Building
Telephone number:	850-245-0517
DOE Helpdesk	850-245-9444
Information Security Management:	850-245-9934 / 850-245-9794

Appendix A

Acceptable Use Policy

Acknowledgement of Compliance with Information Security Policies

I, _____, have read and
(PRINTED OR TYPEWRITTEN NAME OF EMPLOYEE)
understand all of the policies and procedures stated in this document and I acknowledge that failure to comply with these policies and procedures may result in civil liability, disciplinary actions up to and including dismissal, or other sanctions.

_____ _____
Signature of Employee Date

_____ _____
Signature of Supervisor Date