DOEA 420.10
Department of Elder Affairs
Management Information Systems Policy and Procedures

Revised March 17, 2010

Signature Block with Effective Date

Signed	2/12/07
Chuck Corley Interim Secretary, Department of Elder Affairs	Effective Date

Table of Contents

User Policies

Data Protection Policies

Operational Policies

Network Security Policies

Computer Use Policy
(Internet and e-mail)

1.0 Purpose
The purpose of this policy is to establish rules regarding the appropriate use of computer equipment, to include Internet and e-mail.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties, such as, but not limited to, Area Agencies on Aging and vendors. This policy applies to all equipment that is owned or leased by DOEA, and equipment owned or leased by all affiliated third parties that have a legal and/or contractual relationships with the Department .

3.0 Policy
Florida Computer Crimes Act, Chapter 815, Florida Statues, provides that the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information, and the stealing of data from computer files is prohibited. Computer crimes are a violation of the Department's policies and may also result in felony criminal charges.

All Department of Elder Affairs employees or business partners who work with computers or have access to computer information should become familiar with Chapter 815, Florida Statutes, and ask their supervisor for any needed clarification. Only department authorized or approved hardware and software may be used on department computers.

3.1 Electronic Mail (e-mail)
E- mail is an extremely quick and inexpensive method of communication with many benefits and possible risks. This policy describes the efforts by the State Technology Office to address the associated risks. This policy applies to all workers, including employees, contractors and temporaries.

Any electronic mail that is a public record pursuant to Chapter 119, Florida Statutes, should be appropriately maintained or printed and retained in accordance with the record retention guidelines promulgated by the Florida Secretary of State. The content and maintenance of electronic mail is the employee's responsibility.

Access to e-mail service is a privilege, not a right, and entails adherence to State policies, Department policies and procedures, and Federal, State, and local laws or regulations. No employee should have any expectation of privacy as to his or her e-mail usage. The Department reserves the right to inspect any and all files stored in private areas of the network or local systems in order to assure compliance with this policy.

a. Incidental personal purposes: It is permissible to use the e-mail system for incidental personal purposes. However, no such use may violate the Department of Elder Affairs' Policies and Procedures or The State Technology Office Policies and Procedures. Incidental personal purposes do not include uses requiring substantial expenditures of time or uses for profit. The e-mail system is not to be used as a personal bulletin board or message service to advertise the purchase, sale, or offering of commodities such as cars, pets, houses, etc. Department bulletin boards located in break room areas are to be used for these purposes. The e-mail system should not be used to distribute invitations to parties, gatherings or other celebratory events without the approval of your division director.

b. Access by Management: Users of e-mail should recognize that the content of an electronic message sent or received in connection with state business or by utilizing state resources is subject to review by management. While e-mails generated for incidental personal purposes may not be public records, employees should not consider any e-mail to be immune from review by management. To ensure the appropriate use of state resources, management reserves the right to monitor and review all e-mail content and activity without the consent of the employee. However, as a matter of policy, the Department

will not systematically monitor e-mail without sufficient cause to believe that an employee is using state resources inappropriately. In the event a request is made to access or disclose electronic messages of an employee without the consent of the employee, management will give delayed notice to the employee. Notice will be delayed to protect the interests for whom the access was requested.

c. Security Risk: Employees should be aware of the possibility of the introduction of a computer virus or other malicious code through e-mail. Therefore, employees must exercise caution when downloading and using attachments to e-mail and should not download attachments from unfamiliar sources. Additionally, because of the security risk inherent in accessing private e-mail accounts through state resources, employees may not access unauthorized e-mail accounts.

d. Illegal or Wrongful purposes: Employees may not use e-mail to misrepresent any position or endorsement by the Department or any other state office, infringe the copyright or other intellectual property rights of third parties, distribute defamatory fraudulent or harassing messages, or otherwise engage in any illegal or wrongful conduct.

e. Judicial Review: This policy is intended only to improve internal management within state agencies and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity by any party against the State of Florida, its agencies, or instrumentalities, its officers or employees, or any other person.

3.2 Internet Use

The Internet is to be used for reasons that are necessary in the accomplishment of an employee's job assignments. Employees are permitted to briefly visit other non-prohibited Internet sites during non-work time, such as lunch or before or after work hours. Examples are health matters, weather, news, business topics, community activities, career advancement and personal enrichment. It is imperative that common sense is used in viewing non-work related sites and they must not result in any additional cost to the Department.

Employees are not permitted to access, send, store, print or display prohibited material including but not limited to gambling, weapons, drugs, drug paraphernalia, violence, or other illegal activities, sexually explicit materials, or materials that include profane, obscene, or inappropriate language, or racial, ethnic or other discriminatory content.

3.3 More detailed examples of prohibited activities for Internet and E-mail.

- Accessing, receiving, or sending communications (web sites, documents, text, images, audio, video, electronic mail, etc.) that contain profanity, vulgarity, language, sexually explicit or pornographic material that is otherwise inappropriate is prohibited. Supervisory personnel must be notified immediately if any prohibited communications are received.

- Accessing, displaying, storing/copying to any type of storage media (hard drive, floppy drive, zip drive, magnetic tape drive, compact disk, memory, etc.) or printing sexually explicit or pornographic materials, or materials containing profanity, vulgarity, or language that is otherwise inappropriate is prohibited.

- Accessing, displaying, storing/copying to any type of storage media (hard drive, floppy drive, zip drive, magnetic tape drive, compact disk, memory, etc.) and/or printing any harassing materials or materials that are threatening in nature is prohibited.

- Engagement in any illegal activities is prohibited.

- Use of the Internet/electronic mail service for personal gain is prohibited. For example: buying or selling items and/or services on the Internet.

- Sending or forwarding chain letters, or soliciting funds or any items of value for political, charitable (excludes the annual Florida State Employees' Charitable Campaign), religious, or other personal causes is prohibited.

- Using e-mail service to harass, intimidate, or otherwise annoy another employee, individual, business, or organization is prohibited.

- Copying disseminating, or printing copyrighted materials in violation of copyright laws is prohibited.

- Printing material from Internet/e-mail services of a personal nature is prohibited.

- Use of the Internet to provide access to confidential or proprietary information is prohibited. Some information is confidential by law. This included but is not limited to information that requires protection form unauthorized access by legal exemption from the Public Records Act, Chapter 119, Florida Statues.

- Sharing your user-ID or password with others is prohibited.

- The employee is ultimately responsible and held accountable for all activities that occur from his/her user-ID/password. Each employee should obtain his/her own user-ID/password.

- Circumventing or otherwise subverting system and network security measures is prohibited.

- Engaging in any activity that in any way may be harmful to computer systems, hardware or software is prohibited. This includes propagating viruses, disrupting services, and damaging files. All files downloaded from the Internet should be scanned for viruses before use and/or distribution.

- Employees should not respond directly to the originator of offensive e-mail messages. Employees should immediately report the communications to their supervisor and the Information Security Officer in the Division of Information Systems. Specific guidance will be given at that time.

- All messages that are, or appear to be, of a questionable nature, or threaten system harm (including chain letters, virus hoaxes, etc.) should be forwarded immediately to the Division of Information Systems Director

- It is the responsibility of the employee's immediate supervisor to approve and monitor the employee's use of the Internet/e-mail service during working hours. Supervisors may monitor usage by direct observation or review history files through the systems administrator.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Acceptable Use Policy

1.0 Overview

The Florida Department of Elder Affairs' (DOEA) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Department's established culture of openness, trust and integrity. DOEA is committed to protecting customers, employees, partners and the Agency from illegal or damaging actions by individuals, either knowingly or unknowingly.
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the State of Florida. These systems are to be used for business purposes in serving the interests of the State of Florida, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every DOEA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment (software and hardware) at DOEA. These rules are in place to protect the employee and DOEA. Inappropriate use exposes DOEA to risks including virus attacks, compromise of network systems and services, legal issues, and compromise our mission to create an environment that provides choices, promotes independence and enables older Floridians to remain in their communities for a lifetime.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties, such as, but not limited to, Area Agencies on Aging and vendors. This policy applies to all equipment that is owned or leased by DOEA, and equipment owned or leased by all affiliated third parties that have a legal and/or contractual relationship with the Department.

4.0 Policy

4.1 General Use and Ownership

1. While DOEA's IT administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the department's systems remains the property of DOEA.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. DOEA recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see DOEA's Information Sensitivity Policy.
4. For security and network maintenance purposes, authorized individuals within DOEA may monitor equipment, systems and network traffic at any time, per DOEA's Audit Policy.
5. DOEA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by confidentiality guidelines, details of which can be found in DOEA's Information Sensitivity Policy. Examples of confidential information include but are not limited to: Customer names, SSN, address, personal health information, and research data that could identify individual identities. Employees and Agency agents must take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every four months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with DOEA's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a DOEA email address to newsgroups should only be conducted in accordance with an employee's official business duties. A disclaimer stating that the opinions expressed are strictly their own and not necessarily those of DOEA is required.
7. All hosts used by the employee that are connected to the DOEA Internet/Intranet/Extranet, whether owned by the employee or DOEA, shall be continually executing approved virus-scanning software with a current virus database, unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of DOEA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DOEA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DOEA.
2. 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 DOEA or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a DOEA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any DOEA account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to DOEA is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, DOEA employees to parties outside DOEA.
16. Deleting any data that is covered by a records retention requirement.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam), except where required for normal business operations.
2. Personal use of DOEA email systems should be kept to a minimum and should not interfere with regular job responsibilities.
3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4. Unauthorized use, or forging, of email header information.
5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. Use of unsolicited email originating from within DOEA's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DOEA or connected via DOEA's network.
8. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Department of Elder Affairs' (DOEA) and the Area Agencies on Aging's (AAA) entire network. As such, all DOEA employees (including contractors and vendors with access to DOEA's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. This policy is subject to changes in accordance with the State Technology Office policies.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any DOEA facility, has access to the DOEA network, or stores any non-public DOEA information. Sharing of information such as email, calendar and files located on network servers can be granted using proxy rights instead of sharing passwords. The user's supervisor must approve proxy access to his or her data.

4.0 Policy
4.1 General

- All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "pseudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at DOEA. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Elder Affairs", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards
Do not use the same password for DOEA accounts as for other non-DOEA access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various DOEA access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Novell account and a UNIX account.

Do not share DOEA passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential DOEA information. Access to users data can be granted via proxy rights upon request. Proxy rights requires the user's and his or her supervisor's approval. DOEA Division of Information Systems can assist with this request.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss*****
- Don't reveal a password to co-workers while on vacation*****
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don't talk about a password in front of others

***Sharing of information such as email, calendar and files located on network servers can be granted using proxy rights instead of sharing passwords. The user's supervisor must approve proxy access to his or her data.**

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every four months (except system-level passwords which must be changed quarterly).

If an account or password is suspected to have been compromised, report the incident to DOEA and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by DOEA or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the DOEA Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History

Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to the Florida Department of Elder Affairs' (DOEA) network from any host. These standards are designed to minimize the potential exposure to DOEA from damages that may result from unauthorized use of DOEA resources. Damages include the loss of sensitive or agency confidential data, intellectual property, damage to public image, damage to critical DOEA internal systems, etc.

2.0 Scope
This policy applies to all DOEA employees, contractors, vendors and agents with an DOEA-owned or personally owned computer or workstation used to connect to the DOEA network. This policy applies to remote access connections used to do work on behalf of DOEA, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc. Sending e-mail from a third party Internet provider (AOL, MSN, Yahoo, etc.) to a GroupWise account is not considered "remote access" and is therefore not covered under this policy section.

3.0 Policy
3.1 General
1. It is the responsibility of DOEA employees, contractors, vendors and agents with remote access privileges to DOEA's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to DOEA.
2. Please review the following policies for details of protecting information when accessing DOEA's network via remote access methods, and acceptable use of the network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
3. For additional information regarding DOEA's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., contact DOEA MIS

3.2 Requirements
1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any DOEA employee provide their login or email password to anyone, not even family members.
3. DOEA employees and contractors with remote access privileges must ensure that their DOEA-owned or personal computer or workstation, which is remotely connected to DOEA's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. DOEA employees and contractors with remote access privileges to DOEA'S network must not use non-DOEA email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct DOEA business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the DOEA network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by DOEA Division Information Systems.

9. All hosts that are connected to DOEA internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to DOEA's networks must meet the requirements of DOEA-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the DOEA production network must obtain prior approval from DOEA Division of Information Systems.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Cable Modem
Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP
Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem
A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing
Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into DOEA's network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a DOEA-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into DOEA and an ISP, depending on packet destination.

DSL
Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay
A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage.

ISDN
There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access
Any access to DOEA's network through a non-DOEA controlled network, device, or medium.

Split-tunneling

Simultaneous direct access to a non-DOEA network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into DOEA's network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Wireless Communication Policy

1.0 Purpose
This policy prohibits access to the Florida Department of Elder Affairs (DOEA) networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy and have been granted an exclusive waiver by DOEA are approved for connectivity to DOEA networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the DOEA internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the DOEA networks do not fall under the purview of this policy.

3.0 Policy
To comply with this policy, wireless implementations must: Maintain point to point hardware encryption of at least 56 bits. Maintain a hardware address that can be registered and tracked, i.e., a MAC address. Support strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History

Mobile Devices Policy

1.0 Purpose

This policy defines the additional security provisions for mobile device users and the hardware/software used on these devices. This policy is designed to minimize the possibility of loss of sensitive data upon the loss of a mobile device.

2.0 Scope

This policy covers all Mobile computing devices such as laptop computers, handheld devices (e.g. Blackberries, Palm Treos) and mobile storage devices (USB memory or portable disk drives).

3.0 Policy

To comply with this policy, employees using mobile devices must make every effort to protect them from loss or theft, additionally non-agency software or hardware is not to be used on mobile devices. Users must report theft or loss of mobile devices to their supervisor. Additionally the Information Security Officers of the department will be notified

Mobile devices containing confidential information must be encrypted.

Mobile devices must comply with all other security and privacy policies as appropriate.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Mobile Device Encryption	A method by which the contents of a mobile device are protected and are inaccessible to an unauthorized user.

6.0 Revision History

Information Security Policy

1.0 Purpose

The purpose of this information security policy is to protect the information possessed and used by the Department of Elder Affairs (DOEA), whether it is stored in electronic data systems or by any other means. This policy will emphasize guidelines for the protections of the confidential data that are vital to agency operations.

The data security policy is designed to provide a level of confidence that information provided to the Department of Elder Affairs by business partners, contractors and clients will be adequately protected. The Department of Elder Affairs has a responsibility to protect the privacy of our clients by establishing especially stringent protections for client data.

This policy applies to all DOEA employees, contractors and other entities that access the information resources of DOEA including paper documents and electronic data systems.

2.0 Scope

Employees and other users of Information at DOEA have different roles in information security. The responsibilities and procedural guidelines will be organized according to these roles. These guidelines are to assist employees in identifying confidential data and protecting its security. Employees should refer data security questions to their supervisor, who will confer with the appropriate data security officer.

3.0 Policy

Data Confidentiality and Security Guidelines

A. Confidential Client Data – Confidential Client Data is any information electronic or otherwise which identifies an individual client. It addition to the identifying information such as Social Security Number or name, there may be information such as the services the client has received, addresses, or medical and psychosocial assessment information. These data are protected under the Health Insurance Portability and Accountability Act (HIPPA). The department requires training in the security and privacy provisions of HIPPA to all employees.

1. The DOEA Application programs such as CIRTS and CMS have security roles assigned that allow users to view the information required to perform their jobs, while protecting the privacy of our clients. Similar protocols should be adopted by all users of DOEA Confidential Client Data: **Share confidential client information only with persons who need the information to serve the client, and provide only the minimum amount of information required.**
2. Do not leave confidential client information in public view, This applies to paper documents and data on computer screens. **Do not remain logged into client applications such as CIRTS, CMS, or FMMIS when you are not in your office. Do not leave client records or other client specific data in plain view when you are not in your office.**
3. Generally, any information provided to individuals who are not involved in client services should have all identifying information

redacted (obscured or encrypted). **If you receive requests for client information from research organizations or other parties not involved directly in client services, please contact the DOEA Chief Information Officer or General Counsel's Office.**

B. Confidential Data – Confidential Data is distinguished from Confidential Client Data where the person identified is not a DOEA client but is rather an employee, vendor, contractor, volunteer, or other business associate.

1. Share confidential information only with persons who need the information for business purposes, and provide only the minimum amount of information required.
2. Do not leave confidential information in public view, This applies to paper documents and data on computer screens. **Do not leave computers screens or paper documents displaying confidential information unattended.**
3. Any supportive documents intended for MyFlorida Marketplace (MFMP) must have all identifying information obscured (redacted) before being scanned into MFMP.
4. If you need assistance in determining how to handle confidential data, please contact your supervisor, the agency HIPPA Privacy officer, or the Chief Information Officer.

C. Public Records Data – Much of the information possessed by the Department is in the public domain, however there are many important exceptions. The General Counsel's Office makes determinations about what information is a public record under the Sunshine Law and what information is exempt.

1. Copies of available final published documents can be provided upon request.
2. Aggregated research data that do not identify individual clients can be provided upon request.
3. Public records requests other then routine requests for reports as indicated above should be referred to the general counsel's office.
4. Any public record request that identifies individual people, be they clients, employees, vendors, volunteers, or any other person should be referred to the General Counsel's office for approval.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Information User Roles

- **All information Users –** This group includes anyone who interacts with information belonging to the Department of Elder Affairs
- **Chief Information Officer (CIO)–** The Administrator responsible for the coordination of all information technology services including those related to information privacy and security.
- **DOEA Managers –** This role includes DOEA employees who supervise employees using DOEA information. DOEA Managers are responsible to ensure that the employees they manage adequately protect the security of DOEA information.

- **External Information Users / Providers –** This role includes all contractors and subcontractors, service providers, and vendors who use information from or provide information to the Florida Department of Elder Affairs.
- **HIPAA Privacy Officer** – The person responsible for privacy issues related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). At Elder Affairs, this is the General Counsel, and the role extends to privacy issues beyond HIPPA.
- **Information Technology Security Manager (ISM) –** This person is appointed by the CIO to administer the Department's Information Security Program, and to serve as the Department's internal and external point of contact on information security matters. While these duties primarily involve information technology issues they extend to all matters related to information security.

Information Types

- **Manual Data** – Manual Data comprise all data not stored or transmitted electronically. Examples include copies of faxed correspondence, client case files, paper personnel files.
- **Electronic Data –** Electronic Data refers to information that is stored or transmitted electronically. Examples include information in database applications, images of documents, electronic mail messages.
- **Confidential Client Data –** Confidential client data requires the highest level of protection to ensure client privacy. Examples include client assessment data, services provided to clients, and any documents that specifically identify a client.
- **Confidential Data –** Confidential data is data that contains personal identification information. The category includes identification of vendors, subcontractors, and employees. Examples include attachments to vendor invoices, time sheets, and personnel records.
- **Public Record Data –** Data subject to the Florida State Government in the Sunshine Law. This includes most non-client data used in the operation of state agencies. It is generally available to the public upon request. DOEA employees are required to submit any public records requests through the General Counsel's office.

6.0 Revision History

Risk Assessment Policy

1.0 Purpose
To empower the Florida Department of Elder Affairs (DOEA) to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope
Risk assessments can be conducted on any entity within DOEA or any outside entity that has signed a *Third Party Agreement* with DOEA. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy
The execution, development and implementation of remediation programs is the joint responsibility of DOEA and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the DOEA Risk Assessment Team in the development of a remediation plan.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Entity	Any business unit, department, group, or third party, internal or external to DOEA, responsible for maintaining DOEA assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of DOEA's key information assets and systems. DOEA is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

6.0 Revision History

Backup Policy

1.0 Purpose

The purpose of this policy is to establish rules regarding user data backup at the Florida Department of Elder Affairs (DOEA) headquarters.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties that have a legal and/or contractual relationships with the Department.

3.0 Policy

All user data contained on servers located at DOEA Headquarters shall be backed up each weeknight by designated Division of Information Systems' employees. Tapes from these backups will be stored on site for at least one month and one tape from each week will be moved to the DOEA dry storage location and remain there for at least 2 years.

All user data contained on servers located at the Area Agencies on Aging shall be backed up each weeknight by LAN administrators or other designated employees.

The Root of the Novell e-Directory will be backed up monthly. These backups will not be archived.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Data Destruction Policy

1.0 Purpose
The purpose of this policy is to establish rules for the Florida Department of Elder Affairs (DOEA) regarding the destruction of data on equipment or media.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties that have a legal and/or contractual relationship with the Department.

3.0 Policy
1. Confidential information on paper shall be shredded before disposal.

2. When disposing of obsolete computer equipment, ensure that the hard disks are completely wiped of confidential data and proprietary software. Before any computer equipment containing DOEA data is disposed of in any manner, authorization must first be obtained by DOEA's Chief Information Officer (CIO). Verification of complete data "wiping" will be performed and documented.

3. If a disk drive containing confidential data has failed and cannot be overwritten, destroy it physically (e.g., by smashing or incinerating) to prevent uncontrolled data recovery.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Termination/Suspension of Computer Services

1.0 Purpose
The purpose of this policy is to establish rules regarding the suspension of an employee's rights to access all or part of the Florida Department of Elder Affairs (DOEA) network.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties, such as, but not limited to, Area Agencies on Aging and vendors.

3.0 Policy
DOEA Division of Information Systems (DIS) will terminate an employee's user account at the request of the personnel department or the employee's Division Director. The information contained in the user's home directory and e-mail will be maintained for at least one month. Rights to this information will be granted at the request of the employee's supervisors and/or division director. Requests to terminate a current employee's rights to network resources will be accepted form the employee's supervisor and/or division director.

All above requests shall be completed within 24 hours or sooner upon request of the personnel department or the employee's supervisor and/or division director.

3.5 Procedure
Requests for termination or Suspension of Computer Services for a DOEA Computer Service user can be made by the following means:

- Communicated via the Personnel Action Report which is produced and distributed at least weekly by the Personnel office of the Department of Elder Affairs to communicate routine changes in personnel status
- Direct verbal requests by Department Chief of Staff, Division Director, or Bureau Chief to the Chief Information Officer, Information Security Officer or their designee usually in the case of non-routine requests

Actions Taken by the Information Technology Office (or AAA LAN Administrators)

- Change password for Network Access (Novell password)
- Change Password for Electronic Mail (Groupwise password)
- Change Password to the Applications (Oracle Single Sign-On password)
- Verify that each password indicated above has been changed

Information contained in suspended accounts will be maintained for at least one month or as directed by the requestor or agency management. Rights to access these suspended accounts will be granted as directed by the DOEA Computer Service User's division director.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History
Procedure Section added 3-17-2010

Application Service Providers (ASP) Policy

1.0 Purpose
This document describes Information Security's requirements of Application Service Providers (ASPs) that engage with the Florida Department of Elder Affairs (DOEA).

2.0 Scope
This policy applies to any use of Application Service Providers by DOEA, independent of where hosted.

3.0 Policy
3.1 Requirements of Project Sponsoring Organization
The ASP Sponsoring Organization must first establish that its project is an appropriate one for the ASP model, prior to engaging any additional infrastructure teams within DOEA or ASPs external to the agency. The person/team wanting to use the ASP service must confirm that the ASP chosen to host the application or project complies with this policy. The Business Function to be outsourced must be evaluated against the following:

1. The requester must go through the ASP engagement process with DOEA Division of Information Systems (DIS) to ensure affected parties are properly engaged.
2. The ASP must conform and comply with all HIPAA related rules and regulations, including but not limited to, privacy, security, and transaction code sets.
3. In the event that DOEA data or applications are to be manipulated by, or hosted at, an ASP's service, the ASP sponsoring organization must have written, explicit permission from the data/application owners. A copy of this permission must be provided to DOEA.
4. The information to be hosted by an ASP must fall under the "Minimal" or "More Sensitive" categories. Information that falls under the "Most Sensitive" category may not be outsourced to an ASP. Refer to the *Information Sensitivity Policy* for additional details.
5. If the ASP provides confidential information to DOEA, the ASP sponsoring organization is responsible for ensuring that any obligations of confidentiality are satisfied. This includes information contained in the ASP's application. DOEA legal services department should be contacted for further guidance if questions about third-party data arise. Projects that do not meet these criteria may not be deployed to an ASP.

3.2 Requirements of the Application Service Provider
DOEA has created an associated document, entitled *ASP Security Standards* that sets forth the minimum security requirements for ASPs. The ASP must demonstrate compliance with these Standards in order to be considered for use.

The ASP engagement process includes a DOEA evaluation of security requirements. The *ASP Security Standards* can be provided to ASPs that are either being considered for use by DOEA, or have already been selected for use.

DOEA may request that additional security measures be implemented in addition to the measures stated in the *ASP Security Standards* document, depending on the nature of the project. DOEA may change the requirements over time, and the ASP is expected to comply with these changes.

ASPs that do not meet these requirements may not be used for DOEA projects.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Application Service Providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

5.0 Definitions

Terms	Definitions
Application Service Provider (ASP)	ASPs combine hosted software, hardware and networking technologies to offer a service-based application, as opposed to a DOEA-owned and operated application. Common ASP offerings include enterprise resource planning (ERP), collaboration and sales force automation tools, but are not limited to these things.
ASP Sponsoring Organization	The group within DOEA that wishes to utilize the services of an ASP.
Business Function	The business need that a software application satisfies.

6.0 Revision History

Audit Policy

1.0 Purpose
To provide the authority for members of the Florida Department of Elder Affairs (DOEA) Division of Information Systems team to conduct a security audit on any system owned or operated by DOEA.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to DOEA security policies
- Monitor user or system activity where appropriate.

2.0 Scope
This policy covers all computer and communication devices owned or operated by DOEA, including those located at remote locations such as an Area Agency of Aging. This policy also covers any computer and communications device that are present on DOEA premises, but which may not be owned or operated by DOEA.

3.0 Policy
When requested, and for the purpose of performing an audit, any access needed will be provided to members of the DOEA Division of Information team.

This access may include:

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on DOEA equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on DOEA networks.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Automatically Forwarded Email Policy

1.0 Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive information at the Florida Department of Elder Affairs (DOEA).

2.0 Scope
This policy covers automatic e-mail forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of DOEA.

3.0 Policy
Employees must exercise utmost caution when sending any e-mail from inside DOEA to an outside network. Unless approved by an employee's manager, DOEA e-mail will not be **automatically forwarded** to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that e-mail is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Civil and/or Criminal actions may also apply.

5.0 Definitions

Terms	**Definitions**
E-mail	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora, GroupWise and Microsoft Outlook use SMTP.
Forwarded e-mail	E-mail resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to DOEA, its private sector partners or their clients.
Unauthorized Disclosure	The intentional or unintentional revealing of confidential information protected by law.

6.0 Revision History

Continuity of Operations (COOP) Planning

1.0 Purpose
The purpose of this policy is to establish rules a Business Continuity Plan for the Florida Department of Elder Affairs (DOEA) Division of Information Systems.

2.0 Scope
This policy applies to all Elder Affairs employees and affiliates.

3.0 Policy
3.01.1 The COOP Team must identify contingencies that could harm continued operations.

3.01.2 Identify assets of the organization requiring protection in specific contingencies.

3.01.3 Identify and rank in importance the essential functions for continued service to stakeholders.

3.01.4 Define time-limits for recovery of each critical element of operations.

3.01.5 Define, document and test disaster-prevention measures to safeguard each critical element.

3.01.6 Define, document and test disaster-recovery measures for each critical element.

3.01.7 Maintain COOP plan up-to-date as business requirements and processes change over time.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Information Systems Development Methodology (ISDM)

1.0 Purpose
The purpose of this policy is to establish rules regarding Information Systems Development Methodology (ISDM) procedures. Refer to the DOEA Information Systems Development Methodology document for further information.

2.0 Scope
This policy applies to all DOEA employees and affiliates.

3.0 Policy

- Projects vary in size and complexity from a simple single user program that produces a report to a department-wide client services tracking system. The ISDM will be applied with common sense and flexibility to ensure that the benefits gained are proportional to the time and effort required by using it.
- Relatively minor maintenance level activities (code changes) do not require the full-blown use of the ISDM process, but would require the completion of a Technology Support Request Form available at the Information Systems' Help Desk.
- Projects that require more than one division's involvement or where historical documentation is desired, use of the ISDM process would be required. Examples where the ISDM process would be necessary would be the development of new applications or updates of existing applications.
- The Division initiating the request will complete the ISDM Project Proposal Form and submit it to the Division of Information System's (DIS) Help Desk for processing. The request will be logged and then staffed to the appropriate DIS staff member for action
- The Division of Information System's ISDM Team will review the request and complete their portion of the ISDM. At that time, an estimate of resources needed for the project will be determined.
- The ISDM Team Leader will meet with the initiating Division's Coordinator to discuss the request. Recommendations, concerns, and time lines will be discussed at this meeting. It will also be decided as to whether the application or changes will be completed by DIS staff or by an outside contractor.
- After the initiating Division's Coordinator and the DIS ISDM Team have completed the ISDM, it will be forwarded to the appropriate DOEA staff members for review and signatures. Appropriate staff members will include the following:

  Requests with estimated completion dates of < one month, and/or minimal staffing requirements, and/or minimal fiscal impact*:
  - Initiating Division Director
  - Division Director, Information Systems

  Requests with estimated completion dates of > one month, and/or significant staffing requirements, and/or significant fiscal impact*:
  - Initiating Division Director
  - Chief, Decision Support Services
  - Division Director, Administrative Services
  - Deputy Secretary
  - Secretary

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Operating System (OS) Change Control Policy

1.0 Purpose

The purpose of this policy is to establish rules regarding making changes in the Florida Department of Elder Affairs (DOEA) IT system.

2.0 Scope

This policy applies to all DOEA employees and affiliates.

3.0 Policy

1. To the extent possible, all changes to the Operating System (OS) must occur during low-use times such as weekends.

2. Before modifying the OS with additional modules or patches, operations staff must:

    - Install the new software on an isolated system as a trial, whenever feasible.
    - Make two full backups of the entire system.
    - Install the OS from a known-good copy.

3. Immediately after modifying the OS, operations staff must make a known-good copy of the OS.

4. No patch will be installed without verifying its authenticity and integrity (normally by checking the digital signature on a patch program or source code).

5. If a patch or modified module is available as source code, it is preferable to compile the source locally to generate object code for installation.

6. Because the authenticity and integrity of compilers used for generating OS patches and modules is as important as that of the OS itself, compilers shall be reinstalled from known-good copies before compiling OS or patch source code.

7. Full (maximally extensive and detailed) system logging must be enabled during all installation and patch procedures.

8. Working with the quality assurance group, the operations group must define acceptance-testing procedures to determine if the new OS version is allowed to remain on the production system(s).

    - Have representatives of a wide range of users prepare their own tests for the applications they know best.
    - Reload production data that have already been processed and run transaction and report programs again to verify that results are identical before and after the changes to the OS.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Operating System (OS) – The low-level software that handles the interface to peripheral hardware, schedules tasks, allocates storage, and presents a default interface to the user when no application program is running.

6.0 Revision History

Operations Management Policy

1.0 Purpose

The purpose of this policy is to establish rules regarding monitoring of critical IT systems at the Florida Department of Elder Affairs (DOEA).

2.0 Scope

This policy applies to all DOEA employees and affiliates.

3.0 Policy

1. All production systems (including systems used for programming) should be equipped with anomaly detection systems that will notify the system operator (sysop) on duty when anomalies occur.
2. Anomalies include such problems as:

- Running out of disk space
- Failure to mount a required tape within a maximum time limit
- Failure to mount a required printer form or more paper within a maximum time limit
- CPU saturation
- I/O thrashing
- Operating system failure
- Application software failure (e.g., in production batch programs)
- Failure to meet defined system performance or throughput standards
- CPU loop or halt of any kind
- Denial of service attack
- Attempted or successful intrusion (see Intrusion Detection section below).

3. Each sysop on duty must have a fallback staff member whom the anomaly detection system will notify so they can respond to system alerts if the primary sysop cannot respond to the first alert in a timely fashion.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Acceptable Encryption Policy

1.0 Purpose
The purpose of this policy is to provide the Florida Department of Elder Affairs (DOEA) guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal and State of Florida regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties, such as, but not limited to, Area Agencies on Aging and vendors. This policy applies to all equipment that is owned or leased by DOEA, and equipment owned or leased by all affiliated third parties that have a legal and/or contractual relationships with the Department.

3.0 Policy
Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. DOEA key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the DOEA Information Security Officer (ISO). Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Analog/ISDN Line Security Policy

2.0 Purpose
This document explains the Florida Department of Elder Affairs' (DOEA) analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

2.0 Scope
This policy covers only those lines that are to be connected to a point inside a DOEA building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-agency information purposes.

3.0 Policy

3.1 Scenarios & Business Impact
There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside DOEA's premises, then there is the possibility of breaching DOEA's' internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This may potentially result in compromising client information.

The second scenario is the threat of anyone with physical access into a DOEA facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of DOEA through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with the ability to siphon DOEA information to an unknown location. This could also potentially result in the substantial loss of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

3.2 Facsimile Machines
As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a low centralized administrative area designated for departmental use, and away from other computer equipment. The location must be low traffic and not readily accessible to the public or non-departmental employees.
- A computer that is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from DOEA's internal network.
- The line will be used solely for DOEA business, and not for personal reasons.

- All downloaded material, prior to being introduced into DOEA systems and networks, must have been scanned by an approved anti-virus utility (e.g., McAfee VirusScan) which has been kept current through regular updates.

3.3 Computer-to-Analog Line Connections
The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within DOEA will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to DOEA, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case-by-case basis.
Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case-by-case basis.

3.4 Requesting an Analog/ISDN Line
Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom:

- a clearly detailed business case of why other secure connections available at DOEA cannot be used,
- the business purpose for which the analog line is to be used,
- the software and hardware to be connected to the line and used across the line,
- and to what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a DOEA-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from DOEA's' internal network?
- Where will the analog line be placed?
- Is dial-in from outside of DOEA needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a DOEA-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition
Analog - Composed of, or using, continuously changing physical quantities; contrast with digital
ISDN – *(*Integrated Services Digital Network) A high-speed digital network that can carry both voice and data traffic on the same telephone lines.

PBX – (Private Branch Exchange) A telephone exchange local to a particular organization who use, rather then provide, telephone services. The earliest were manual (Private Manual Branch Exchange PMBX) but are now more likely to be automatic (Private Automatic Branch Exchange).
Ethernet connection – A widespread networking scheme most commonly known as "the hardware device that enables the LAN to work at the office."

6.0 Revision History

Anti-Virus Policy

1.0 Purpose

The purpose of this policy is to establish rules regarding anti-virus software on all computer and network equipment owned by the Florida Department of Elder Affairs (DOEA).

2.0 Scope

This policy applies to all DOEA employees and affiliates.

3.0 Policy

- Always run the agency standard, supported anti-virus software is available from the Intranet download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in accordance with DOEA's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab-testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition

***Anti-Virus software* –** A utility program designed to detect and destroy computer viruses.

***Virus* –** A computer program or program segment that can attach itself to another program, reproduce itself, and spread from one program to another. Viruses, which are illegal, are often destructive, changing data and in other ways sabotaging computer systems.

6.0 Revision History

ASP Security Standards

1.0 Overview

This document defines the minimum-security criteria that an Application Service Provider (ASP) must meet in order to be considered for use by the Florida Department of Elder Affairs (DOEA). An example of an ASP would be a web site hosted by a third party or an application used by DOEA that was developed by a third party and hosted by a third party. In each of these examples, DOEA would have a contractual arrangement with the ASP that covered, among other things, HIPAA requirements. As part of the ASP selection process, the ASP Vendor must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the six categories. DOEA Information Systems will closely review the vendor responses, and will suggest remediation measures in any areas that fall short of the minimum security criteria DOEA Information Systems approval of any given ASP resides largely on the vendor's response to this document.

These Standards are subject to additions and changes without warning by DOEA.

2.0 Scope

This document can be provided to ASPs that are either being considered for use by DOEA, or have already been selected for use.

3.0 Responding to These Standards

DOEA is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each Guideline should be specific and avoid generalities, e.g.:

Examples:

Unacceptable: "We have hardened our hosts against attack."
Acceptable: "We have applied all security patches for Windows 2000 as of 8/31/2000 to our servers. Our Administrator is tasked with keeping up-to-date on current vulnerabilities that may affect our environment, and our policy is to apply new patches during our maintenance period (2300hrs, Saturday) every week. Critical updates are implemented within 24 hours. A complete list of applied patches is available to DOEA."

Unacceptable: "We use encryption."
Acceptable: "All communications between our site and DOEA will be protected by IPSec ESP Tunnel mode using 168-bit TripleDES encryption, SHA-1 authentication. We exchange authentication material via either out-of-band shared secret, or PKI certificates."

4.0 Standards

4.1 General Security

1. DOEA reserves the right to periodically audit the DOEA application infrastructure to ensure compliance with the ASP Policy and these Standards. Non-intrusive network audits (basic portscans, etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 24 hours notice.

2. All Application Service Providers must comply with all HIPAA rules and regulations, including but not limited to security, privacy, and transaction code sets.

3. The ASP must provide a proposed architecture document that includes a full network diagram of the DOEA Application Environment, illustrating the relationship between the Environment and

any other relevant networks, with a full data flowchart that details where DOEA data resides, the applications that manipulate it, and the security thereof.

4. The ASP must be able to immediately disable all or part of the functionality of the application should a security issue be identified.

4.2 Physical Security

1. The equipment hosting the application for DOEA must be located in a physically secure facility, which requires badge access at a minimum.

2. The infrastructure (hosts, network equipment, etc.) hosting the DOEA application must be located in a locked cage-type environment.

3. DOEA shall have final say on who is authorized to enter any locked physical environment, as well as access the DOEA Application Infrastructure.

4. The ASP must disclose who amongst their personnel will have access to the environment hosting the application for DOEA.

5. DOEA's Asset Protection team requires that the ASP disclose their ASP background check procedures and results prior to DOEA granting approval for use of an ASP.

4.3 Network Security

1. The network hosting the application must be air-gapped from any other network or customer that the ASP may have. This means the DOEA application environment must use separate hosts, and separate infrastructure.

2. How will data go between DOEA and the ASP? Keep in mind the following two things:

   a. If DOEA will be connecting to the ASP via a private circuit (such as frame relay, etc.), then that circuit must terminate on the DOEA extranet, and the operation of that circuit will come under the procedures and policies that govern the DOEA extranet.

   b. If, on the other hand, the data between DOEA and the ASP will go over a public network such as the Internet, appropriate firewalling technology must be deployed by the ASP, and the traffic between DOEA and the ASP must be protected and authenticated by cryptographic technology (See Cryptography below).

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Unix, NT, etc.) comprising the DOEA application infrastructure have been hardened against attack. If the ASP has hardening documentation for the CAI, provide that as well.

2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.

3. Information on how and when security patches will be applied must be provided. For example, we would need to know how the ASP keeps current on security vulnerabilities, and what is their policy for applying security patches?

4. The ASP must disclose their processes for monitoring the integrity and availability of those hosts.

5. The ASP must provide information on their password policy for the DOEA application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.

6. DOEA cannot provide internal usernames/passwords for account generation, as the agency is not comfortable with internal passwords being in the hands of third parties. With that restriction, how will the ASP authenticate users? (e.g., LDAP, Netegrity, Client certificates.)

7. The ASP must provide information on the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

1. At DOEA's discretion, the ASP may be required to disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases).

2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP (active server page) technology.

3. What language is the application back-end written in? (C, Perl, Python, VBScript, etc.)

4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.

5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

1. The DOEA application infrastructure cannot utilize any "homegrown" cryptography – any symmetric, asymmetric or hashing algorithm utilized by the DOEA application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic community.

2. Encryption algorithms must be of sufficient strength to equate to 168-bit TripleDES.

3. Preferred hashing functions are SHA-1 and MD-5.

4. Connections to the ASP utilizing the Internet must be protected using any of the following cryptographic technologies: IPSec, SSL, SSH/SCP, PGP.

5. If the DOEA application infrastructure requires PKI, please contact DOEA Information Systems for additional guidance.

5.0 Definitions
Term Definition

Application Service Provider – A service (usually a business) that provides remote access to an application program across a network protocol, typically HTTP. A common example is a web site that other web sites use for accepting payment by credit card as part of their online ordering systems.

HIPAA – ***Health Insurance Portability and Accountability Act of 1996***. HIPAA is a broad federal law that addresses many healthcare issues, including insurance benefits, medical savings accounts, and fraud and abuse.

Cryptography – The practice and study of encryption and decryption – encoding data so that it can only be decoded by specific individuals.

Patches – Temporary addition to a piece of code, usually as quick-and-dirty remedy to an existing bug or misfeature.

6.0 Revision History

Dial-In Access Policy

1.0 Purpose
The purpose of this policy is to protect the Florida Department of Elder Affairs' (DOEA) electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

2.0 Scope
The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3.0 Policy
DOEA employees and authorized third parties can use dial-in connections to gain access to the network. The dial-in access uses a one-time password authentication. Dial-in access should be strictly controlled and users must have their Director's approval. Applications for a dial-in account can be obtained at the DOEA Information Systems Help Desk. The DOEA Information Systems Director must approve all applications.

It is the responsibility of users with dial-in access privileges to ensure a dial-in connection to DOEA is not used by non-authorized users to gain access to agency information system resources. A user who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and DOEA are literal extensions of DOEA's network, and that they provide a potential path to the agency's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect DOEA's assets.

Analog and non-GSM digital cellular phones cannot be used to connect to DOEA's network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to DOEA's network. For additional information on wireless access to the DOEA network, consult the *Wireless Communications Policy*.

Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition
Dial-in – To connect to the network using a telephone line or dial-up method.
Analog - Composed of, or using, continuously changing physical quantities; contrast with digital.
GSM digital cellular phone – (Global Standard for Mobile Communication) The dominant set of standards used in Europe and parts of Asia for wireless communications.

6.0 Revision History

DMZ Lab Security Policy

1.0 Purpose

This policy establishes information security requirements for all networks and equipment deployed in the Florida Department of Elder Affairs (DOEA) labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to DOEA from the damage to public image caused by unauthorized use of DOEA resources, and the loss of confidential data.

2.0 Scope

DOEA Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside DOEA Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside DOEA's Internet firewalls.

3.0 Policy

3.1. Ownership and Responsibilities

1. All new DMZ Labs must present a business justification with sign-off at the business unit Vice President level. DOEA must keep the business justifications on file.
2. Lab owning organizations are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must maintain up to date POC information with DOEA. Lab managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through DOEA Information Systems and approved by DOEA.
4. All ISP connections must be maintained by DOEA Information Systems.
5. A Network Support Organization must maintain a firewall device between the DMZ Lab(s) and the Internet.
6. The Network Support Organization and DOEA reserve the right to interrupt lab connections if a security concern exists.
7. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the Network Support Organization point of demarcation.
8. The Network Support Organization must record all DMZ Lab address spaces and current contact information.
9. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of DOEA and the Network Support Organization upon request, in accordance with the *Audit Policy*
11. Individual lab accounts must be deleted within three (3) days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) days from a change in the group membership.
12. DOEA will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to DOEA's internal networks, either directly or via a wireless connection.
3. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
4. Lab Managers are responsible for complying with the following related policies:
    a. *Password Policy*
    b. *Wireless Communications Policy*

c. **Lab Anti-Virus Policy**

5. The Network Support Organization maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs. All firewall filters will be maintained by DOEA.
6. The firewall device must be the only access point between the DMZ Lab and the rest of DOEA's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by DOEA (including both general configurations and rule sets). DOEA may require additional security measures as needed.
8. Traffic from DMZ Labs to the DOEA internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards. [Add url link to site where your internal configuration standards are kept].
11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not serving business requirements must be disabled.
14. DOEA Confidential information is prohibited on equipment in labs where non-DOEA personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy*
15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ (de-militarized zone)	Networking that exists outside of DOEA primary firewalls, but is still under DOEA administrative control.
Network Support Organization	Any DOEA-approved support organization that manages the networking of non-lab networks.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
Network Support Organization Point of Demarcation	The point at which the networking responsibility transfers from a Network Support Organization to the DMZ Lab. Usually a router or

	firewall.
Lab Manager	The individual responsible for all lab activities and personnel.
Lab	A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
Firewall	A device that controls access between networks., such as a PIX, a router with access control lists, or a similar security device approved by DOEA.
Internally Connected Lab	A lab within DOEA's firewall and connected to the production network.

6.0 Revision History

File and Print Server Policy

1.0 Purpose
The purpose of this policy is to establish rules regarding file and print servers located at the Florida Department of Elder Affairs (DOEA) offices.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties that have a legal and/or contractual relationships with the Department.

3.0 Policy

1. Desktop PCs set up for file sharing are treated the same as a server and will be configured to meet all required security initiatives by either DOEA Information Systems personnel or the Area Agencies on Aging LAN Administrators, where applicable.

2. Approval for file and print servers must be approved by DOEA's Director of Information Systems via an e-mail request. Required documentation justifying this request must remain on file within the Information Systems Division. Request forms are available at the Help Desk.

3. Run AV Scanner in full time, background, automatic, auto-protect or similar mode on any file server which potentially stores files that are potentially infect-able such as*.doc files and executables that run on desktops.

4. Update server signature files monthly if alert service is available, weekly (or at maximum vendor rate) if no alert service is available.

5. File and Print servers must utilize centralized AV management.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition
AV Scanner – An input device that takes in an optical image and digitizes it into an electronic image represented as binary data. This can be used to create a computerized version of a photo or illustration.

6.0 Revision History

Firewall Policy

1.0 Purpose

The purpose of this policy is to establish rules regarding firewall protection of the Florida Department of Elder Affairs (DOEA) network. This policy is subject to change in accordance with the State Technology Office's security policies.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties, such as, but not limited to, Area Agencies on Aging and vendors. This policy applies to all equipment that is owned or leased by DOEA, and equipment owned or leased by all affiliated third parties that have a legal and/or contractual relationships with the Department.

3.0 Policy

1. Include all modes of network access in your Network Service Access Policy, including TCP/IP, dial-in and SLIP/PPP connections.

2. Balance functional requirements of your staff with security considerations; draconian restrictions that prevent people from getting their work done will be circumvented.

3. Use a restrictive policy for firewall parameters so that all services are denied unless specifically permitted.

4. If different user communities require radically different firewall policies, segregate the more permissive users on a subnet with appropriate access parameters but screen that subnet to prevent access to more secure parts of the network.

5. Block all inbound and outbound use of the following services:
    - Trivial FTP (TFTP) on port 69
    - X-Windows on ports 6000+ and OpenWindows on port 2000
    - Remote Procedure Call (RPC) on port 111
    - Rlogin, rsh and rexec on ports 513, 514, and 512 respectively

6. Restrict the following services to systems that need them:
    - TELNET on port 23
    - FTP on ports 20 and 21
    - SMTP on port 25
    - RIP (routing information protocol) on port 520
    - DNS on port 53
    - UUCP on port 540
    - NNTP on port 119
    - Gopher on port 70
    - HTTP on port 80

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition

Firewall
TCP/IP connections
SLIP/PPP connections

6.0 Revision History

Router Security Policy

1.0 Purpose
This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the Florida Department of Elder Affairs (DOEA).

2.0 Scope
All routers and switches connected to DOEA production networks are affected. Routers and switches within internal, secured labs are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

3.0 Policy
Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use TACACS+ for all user authentication.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    a. IP directed broadcasts
    b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
    c. TCP small services
    d. UDP small services
    e. All source routing
    f. All web services running on router
4. Use agency standardized SNMP community strings.
5. Access rules are to be added as business needs arise.
6. The router must be included in the DOEA network topology with a designated point of contact.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms
Production Network
The "production network" is the network used in the daily business of DOEA. Any network connected to the agency network, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to DOEA employees or impact their ability to do work.

Lab Network
A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to DOEA nor affect the production network.

6.0 Revision History

Screen Security Policy

1.0 Purpose
The purpose of this policy is to establish rules regarding screen saver use on all DOEA owned machines.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties that have a legal and/or contractual relationships with the Department.

3.0 Policy

1. Screen savers are installed and active on all desktop PCs.

2. Screen Saver timeout capability is ENABLED.

3. The enabled timeout is set for 15 minutes or less.

4. Password protection for screen savers is ENABLED.

5. A strong password is enabled on the screen saver.

6. DOEA Division of Information Systems staff and the Area Agencies on Aging LAN Administrators will facilitate the installation process.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition
Screen saver – **Program that displays either a completely black image or a constantly changing image on a computer monitor to prevent a stationary image from "burning" into the phosphor of the screen. Screen savers usually start automatically after the computer has had no user input for a preset time.**
***ENABLED* –** To permit the user to utilize a specific feature or function.

6.0 Revision History

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the Florida Department of Elder Affairs (DOEA). Effective implementation of this policy will minimize unauthorized access to DOEA proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by DOEA (including those located at remote locations such as Area Agencies on Aging), and to servers registered under any DOEA-owned internal network domain.

This policy is specifically for equipment on the internal DOEA network.

3.0 Policy

3.1 Ownership and Responsibilities
All internal servers deployed at DOEA must be owned by an operational group that is responsible for system administration. An Area Agency on Aging is an example of an operational group. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by DOEA. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by DOEA.

- Servers must be registered with DOEA Division of Information Systems. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines
- Operating System configuration should be in accordance with approved DOEA guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows. These audits will be conducted by the LAN Administrators at the AAA level as well as by the DOEA Monitoring Team during period monitoring visits.
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to DOEA, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within DOEA.
- Audits will be managed by the internal audit group or DOEA, in accordance with the *Audit Policy*. DOEA will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	De-militarized Zone. A network segment external to the production network.
Server	For purposes of this policy, a Server is defined as an internal DOEA Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

Virtual Private Network (VPN) Policy

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Florida Department of Elder Affairs (DOEA) network.

2.0 Scope
This policy applies to all DOEA employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the DOEA network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy
Approved DOEA employees and authorized third parties (partners, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to DOEA internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the DOEA network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by DOEA network operational groups.
6. All computers connected to DOEA internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the agency standard; this includes personal computers.
7. VPN users will be automatically disconnected from DOEA’s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not DOEA-owned equipment must configure the equipment to comply with DOEA's VPN and Network policies.
10. Only DOEA-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of DOEA's network, and as such are subject to the same rules and regulations that apply to DOEA-owned equipment, i.e., their machines must be configured to comply with DOEA's Security Policies.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
IPSec Concentrator	A device in which VPN connections are terminated.

6.0 Revision History

Web Server Policy

1.0 Purpose
The purpose of this policy is to establish rules regarding Web servers existing and web sites hosted on equipment located on the Florida Department of Elder Affairs (DOEA) network.

2.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other DOEA workers, including all personnel affiliated with third parties that have a legal and/or contractual relationships with the Department.
3.0 Policy

User
Users are forbidden to download, install or run Web server software.

Network traffic will be monitored for unapproved Web servers, and operators of those servers will be subject to disciplinary action.

Manager
The CIO must approve the operation of any web server to be connected to the Internet in writing.

All content on Agency WWW servers connected to the Internet must be approved by the CIO and the Area Agency on Aging Directors, where applicable, and installed by the designated DOEA or AAA Web Master.

No confidential material may be made available on the Web site.

Information placed on the Web site is subject to the same Privacy Act restrictions as when releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information.

All publicly accessible Web sites must be thoroughly tested to ensure all links work as designed and are not "under construction" when the site is opened to the public. Under construction areas are not to appear on publicly accessible Web sites.

Technical

The Web server software, and the software of the underlying operating system, shall contain all manufacturer recommended patches for the version in use.

All Web sites may be monitored as part of the agency's network administration function. Any user suspected of misuse may have all their transactions logged for possible disciplinary action.

The implementation and use of CGI scripts shall be monitored and controlled. CGI scripts shall not accept unchecked input. Any programs that run externally with arguments should not contain metacharacters. The developer is responsible for devising the proper regular expression to scan for shell metacharacters and shall strip out special characters before passing external input to the server software or the underlying operating system.

All agency WWW servers connected to the Internet will have a firewall between the Web server and internal networks. Any internal WWW servers supporting critical applications must be protected by

internal firewalls. Sensitive, confidential, and private information should never be stored on an external WWW server.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition

Web server – A server process running at a web site which send out web pages in response to HTTP requests from remote browsers.

Network traffic – Communication between workstation and network.

CIO – Chief Information Officer

CGI scripts - A program running on a web server to produce dynamic content, usually an HTML web page, in response to a user's request.

WWW – (World Wide Web) An Internet client-server hypertext distributed information retrieval system which originated from the CERN High-Energy Physics laboratories in Geneva, Switzerland.

5.0 Revision History