# STATE OF ARKANSAS

Department of Veterans Affairs
501 Woodlane Drive Suite 230C
Little Rock, Arkansas 72201
(501) 683-1386 / FAX (501) 682-4833

**Asa Hutchinson**
**Governor**

**Matt Snead**
**Director**

PERSONNEL

ADVAP 2-22 May 1, 2016

## Internet, E-Mail, General Computer, and Cell Phone Use

1. **General:** This policy covers the management of all electronic mail and Internet systems provided by the Department of Finance and Administration. The Department of Finance and Administration encourages the use of the Internet (including electronic mail) as an integral part of its overall processes. Use of the Internet is encouraged to:

a. Provide an efficient method to exchange information within state agencies, between governmental agencies, and with the public;

b. Provide sources of data to assist state employees in accomplishing their tasks;

c. Accomplish the business of government.

2. **Purpose**: To ensure that the use of email and internet activities do not negatively impact the confidentiality, availability, integrity, and reputation of the Arkansas Department of Veterans Affairs (ADVA) and its assets; and to ensure compliance with all applicable federal and state laws.

3. **Philosophy**: It is ADVA's position that an authorized user's access to the Internet and/or email services for limited personal use is a privilege that, if not properly monitored and controlled, could result in harm to the organization or violations of certain federal and state laws. The primary use of these services is for business and clinical purposes and thus need to be appropriately protected. All email correspondence stored in the State's email system is subject to the Arkansas Freedom of Information Act (FOIA)

4. **Applicability**: This standard applies to all ADVA Covered Entities (ASVC-NLR, ASVC-B, ASVH-F, ASVH-NLR, ADVAcates network, ADVA administrative offices and other ADVA entities that may be added from time to time). For purposes of this policy, ADVA Covered Entities shall be collectively referred to as "ADVA".

**5. Acceptable/Unacceptable Use**: The computer system and network are intended for the business use of the employee. Inappropriate or unacceptable use by an employee is basis for disciplinary action. It is unacceptable for a user to use, submit, publish, display, or transmit on the network or on any computer system any information which:

a. Violates or infringes on the rights of any other person, including the right to privacy;

b. Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;

c. Restricts or inhibits other users from using the system(s). Or, use that degrades the efficiency of the computer system(s) such as unofficial: memberships in chat rooms; channel subscriptions; or receipt of streaming or broadcast audio or video. See paragraph 6 for definitions.

d. Uses the system for any illegal purpose or for personal gain.

Only authorized software may be installed on state-owned or leased hardware. In order to guarantee compliance with copyright laws and ensure compatibility with office computer environments and “standard” software loads, the installation of any personally owned or downloaded software/shareware must be preapproved by a System Administrator or your supervisor.

**6. Transmission of personal data/correspondence related to employee disciplinary actions:** In order to protect ADVA employees, contractors, and FVH residents’ personal data, the following types of correspondence and documentation must be sent in an encrypted/password protected format, or faxed:

a. Any that contains the personal data of ADVA employees, contractors or residents of FVH.
b. Any related to employee disciplinary actions.

Personal data includes:

- Social security number;
- Driver’s license number;
- Nursing or other license numbers;
- Personal phone numbers;
- Personal addresses;

- Any other data that can be used to identify an individual that is personal in nature

Multiple documents may be encrypted by copying them into a .zip or similar file and encrypting/password protecting the file. MS-Office applications and Adobe Acrobat include security features that allow the password protection of individual files.

Corresponding passwords may not be sent via email. Call the receiver of the information and provide them the password over the phone.

Violations of this policy are cause for disciplinary action.

7. **Electronic Mail [E-MAIL] and Freedom of Information Act [FOI]:** E-mail is considered network activity; thus, it is subject to all policies regarding acceptable/unacceptable use of state owned or leased computer systems and networks. The user should not consider e-mail to be either private or secure.

a. Personnel shall not use ADVA resources to view, record, or transmit materials which violate ADVA policies. Inappropriate messages, pictures, and/or other visual images/materials include, but are not limited to:

1) Any activity covered by inappropriate use statements included in this policy.

2) Sending / forwarding chain letters, virus hoaxes, urban legends, etc.

3) Fraudulent messages - Messages sent under an anonymous or assumed name with the intent to obscure the origin of the message.

4) Harassment messages - Messages that harass an individual or group for any reason, including race, sex, religious beliefs, national origin, physical attributes, or sexual preference.

5) Obscene messages - Messages that contain obscene or inflammatory remarks.

6) Pornographic materials -This includes, but is not limited to pictures, audio/video files, literature, or newsgroups.

7) Users shall not engage in spamming activities. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.

8) Users shall not photograph, post, or transmit patient images, electronically or otherwise, without a signed consent.

9) Users shall not share sensitive information or protected health information (PHI) on public web sites (i.e., Google Apps, DropBox.com, GoogleDocs, iCloud, etc.) or with persons or entities not specifically authorized to receive the sensitive or protected health information.

10) Users shall not forward email containing sensitive information or protected health information (PHI) to public email systems such as Hotmail.com, gmail.com, or other public email system services. In addition, users shall not forward sensitive information, PHI, or other ADVA business information to their personal email accounts. Personal email accounts shall not be used for official ADVA business.

11) Users shall not knowingly download non-work-related executable files from the Internet.

12) Users shall not misuse their Internet privileges, i.e., spending excessive time on the Internet for non-work related business or accessing inappropriate sites.

13) Users shall not misuse their email privileges, i.e., sending and forwarding non-business related mass emails.

14) Users shall not establish peer-to-peer connections to external parties for file sharing, downloading music and movies, and accessing adult materials.

15) Users shall not knowingly enable an external/remote party to gain unauthorized access or control of any device, application, or system to the data networks.

Because electronic messages are typically stored in one place and then forwarded to one or more locations, often without the specific knowledge of the originator, they are vulnerable to interception or unintended use. ADVA will attempt to provide an electronic messaging environment that provides data confidentiality and integrity. However, ADVA cannot be responsible for web-based e-mail systems such as Yahoo, Juno, etc. State employees should always be aware of the risks associated with the use of all e-mail systems.

b. The Arkansas Freedom of Information Act

The electronic files, including e-mail files, of state employees are potentially subject to public inspection and copying under the state Freedom of Information Act ("FOI"), Ark. Code Ann. § 25-19-101 et seq. The FOI defines "public records" to include "data compilations in any form, required by law to be kept or otherwise kept, which constitute a record of the performance or

lack of performance of official functions which are or should be carried out by a public official or employee [or] a governmental agency. . . ." Ark. Code Ann. § 25-19-103(1). All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records. Various exceptions apply. See Ark. Code Ann.§ 25-19-105, including Ark. Code 26-18-303 which removes state tax records from FOI, Ark. Code 27-50-907 which prohibits release of any personal information concerning a driver, Ark Code 9-14-210 which prohibits releasing child support information and the Federal Driver Privacy Protection Act.

c. Records Retention Policies

All relevant records retention policies and statutes must be followed, and it is the responsibility of each State Employee to understand which of these pertain to his or her work.

d. Maintaining E-Mail

1) ADVA maintains e-mail backups with history up to six months. The responsibility lies with the user for e-mail retention beyond six months. E-mail messages of only transitory value should not be saved. In fact, the failure to routinely delete these messages clogs information systems and strains storage resources.

2) If a user chooses to retain e-mail, that user must understand that all retained files and electronic messages may be accessible under FOI law. In order to properly maintain e-mail using Outlook/Exchange, users must transfer any information they wish to retain to "Personal Folders" on their local hard drive. Users should then empty all messages from their Inbox, Sent Mail folder, and Deleted Items folder. Users should also empty their "Recycle Bins" on a regular basis.

e. Guidelines for effective and efficient use of E-Mail

1) Mail Recipients

a) Prioritize your messages. Don’t automatically respond to e-mails in the order you receive them.

b) Handle urgent and easy to answer ones first. You don’t need to answer everything.

c) Look at the subject line and sender. If you don’t know the sender or the subject line doesn’t apply to you opening the e-mail may just generate more unwanted e-mail.

d) Respond promptly to essential e-mail. If you can't answer a business question quickly let the sender know you received the e-mail and set a timeframe for response.

e) Learn your e-mail program and its capabilities.

2) Mail Senders

a) Always write a definitive subject line. This helps your receiver prioritize their mail.

b) Tailor the text for easy understanding and response.

c) Don't use e-mail for debate

d) Minimize attachments.

e) Keep paragraphs short and to the point.

f) Focus on one subject per message.

g) Use your signature at the bottom of messages when communicating with people who may not know you personally

h) Capitalize words only to highlight an important point. Capitalizing whole words that are not titles is considered as SHOUTING!

i) Asterisks surrounding a word can be used to make a stronger point.

j) Because of the international nature of the Internet, use a date convention spelling out the month and using the full year.

k) Follow chain of command procedures when corresponding with superiors. Don't send a complaint to the "top" just because you can.

3) All Users

a) Delete unwanted messages immediately

b) Keep messages remaining in your mailbox to a minimum

c) Never assume your e-mail can't be read by others

d) All email messages, documents, and correspondence and data obtained via internet use are considered ADVA property.

e) Users shall have no expectation of privacy in email and internet use. ADVA may monitor messages and internet use without prior notice.

f) Users are responsible for reporting any suspected or confirmed violations of this policy to their department manager or to the ADVA Assistant Director.

g) Users shall delete chain and junk email messages without forwarding or replying to them. Electronic chain letters and other forms of non-business related mass mailings are prohibited.

h) ADVA reserves the right to block access to non-business-related material.

i) Email transmission of PHI when necessary shall be conducted with the highest level of security applied and only in situations where the email is necessary for the treatment of the patient, payment, and health care operations. PHI and other sensitive information shall be encrypted during transmission over the Internet (outside ADVA and the State network).

j) Users shall honor all rules of copyright and personal property.

k) Users shall check their email regularly and delete unneeded email.

l) Users shall delete, without opening, suspicious, unsolicited email messages from outside ADVA, especially if they contain attachments with ".exe" file extensions. If a user is receiving repeat emails of this nature, the activity should be reported to ADVAFiscal@arkansas.gov.

m) The use of any software or service that hides the identity of the user or the location of the user while using the Internet is prohibited.

n) Only individuals with administrative responsibilities (i.e., Department Managers, Directors, etc.) or their designee may be granted access to the email account of their former employee or vendor. This may require written approval from requestor's supervisor.

    a. The account shall be used only for the retrieval of existing email and shall not be used to impersonate the former personnel or send email communications.
    b. Access shall be granted for a specific period of time subject to approval by the agency Director.

8. **Privacy of Electronic Records**

a. A system administrator is any person designated by the Department Director to maintain, manage, and provide security for shared multi-user computing resources, including computers, networks, and servers.

b. System Administrators shall perform their duties fairly, in cooperation with the user community and ADVA administrators. They shall adhere to this code and all other pertinent rules and regulations, shall respect the privacy of users to the greatest extent possible, and shall refer disciplinary matters to appropriate ADVA staff.

c. Given the nature of the technology, a wide range of information can be easily collected by ADVA personnel using system software. For example, software may be configured to provide aggregate information on the number of users logged in, the number of users accessing certain software, etc.

d. No information shall be routinely collected that is not required by system administrators in the direct performance of their duties, such as routine backup for system recovery.
e. Unauthorized access to any information will result in immediate disciplinary action.

9. **Regulation / Enforcement:** In order for anyone to gain access to a state employee's e-mail, Internet cache or files without that employee's permission for any reason, the Director of the Department of Finance and Administration (or designee) must submit a signed statement authorizing such access to the appropriate System Administrator.

a. Violation of this policy will result in appropriate disciplinary action to the employee per Administrative Memorandum 300.12. The disciplinary action could result in immediate dismissal.

b. All federal and state laws, as well as general ADVA regulations and policies, are applicable to the use of computing resources. These include, but are not limited to, the Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 et seq.; the Arkansas Freedom of Information Act, Ark. Code Ann. § 25-19-101 et seq.; and state and federal computer fraud statutes, 18 U.S.C. § 1030 and Ark. Code. Ann. § 5-41-101 et seq. Illegal reproduction of software and other intellectual property protected by U.S. copyright laws and by licensing agreements may result in civil and criminal sanctions.

10. **Security:**

a. Email Security:

1. Consider whether the content of the email should be encrypted or password protected.
2. When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.

c. If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

d. Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

e. If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.

b. Fax security

1. Consider whether sending the information by a means other than fax is more appropriate.
2. Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
3. Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
4. If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
5. Call or email to make sure the whole document has been received safely.

f. Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

c. Other security measures

1. When discarding papers that contain confidential information, place in confidential paper shredding and recycling bin. Do not place paperwork that contains confidential information in the trash bin.

2. Use strong passwords - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
3. Do not to send offensive emails about other people, their private lives or anything else that could bring our organization into disrepute. Do not "say" anything in email that you would not like to hear read aloud in a court of law.
4. Do not believe emails that appear to come from your bank or an ADVA bank that ask for account information, credit card details or your password (a bank would never ask for this information in this way);
5. Do not open or forward email that appears to be spam – not even to unsubscribe or ask for no more mailings. Delete the email.

11. **Cell Phone Use:**

a. Cell phones shall be turned off or set to silent or vibrate mode during your work schedule.
b. Employees may carry and use personal cell phones while at work on a sporadic basis. If employee use of a personal cell phone causes disruptions or loss in productivity, the employee may become subject to disciplinary action.

**ASVH-F Cell Phone Use:**

a. All nursing personnel other than listed below must have their cell phones turned off or set to silent or vibrate mode during your work schedule. Cell phones will not be carried on the person and must be locked in a locker or not brought into the building.
b. LPN's may lock their cellphones in the medicine cart for use as needed to contact medical personnel.
c. RN's may carry their cellphone for use to contact medical personnel however personal calls may not be made unless on break in a private area.
d. The DON, and ADON may carry their cellphone anywhere and at anytime.
e. Business Office Personnel may have their cellphones if set to vibrate or silent mode during your work schedule.
f. Cellphones may be used during break times only and in a private area. Cellphones cannot be used in public areas during breaks.
g. During an emergency the employee may be contacted by calling the main line at 479-444-7001. Cellphones will not be allowed on the person for emergency situations.
h. Any unauthorized use of carrying their cell phone may result in disciplinary action.

12. **Definitions:**

a. Channel Subscriptions: Subscribed to services, which provide a continuous flow of updated information such as stock market activity or general world news to a client's desktop computer. Channel Subscriptions are usually activated at the time the desktop system is turned on, at the start of a workday, and may remain active throughout the workday.

b. Chat Rooms: On Line interactive communications, by keyboard, between two or more people using their desktop computers to carry on conversations through the Internet, an on line service, or a Bulletin Board. This is the desktop computer version of a telephone conversation between two people, or, a conference call involving groups of people.

c. Streaming Audio/Video: Audio or video transmission over a data network. The transmissions are received as a continuous stream of audio, such as music files; or video, such as movies, from a provider to the client's desktop computer. The desktop computer is effectively being used in a fashion similar to a radio or television.

d. Urban Legends: Similar to virus hoaxes. Popular narratives alleged to be true, transmitted from person to person by oral, written, or electronic communication (including fax and email). These stories always involve some combination of outlandish, humiliating, humorous, terrifying, or supernatural events – events that always happened to someone else. For credibility, the teller of an urban legend relies on citing of an "authoritative" word-of-mouth source (typically "a friend of a friend") rather than verifiable facts. And sometimes, but not always, there's a moral to the story, e.g.: "behave yourself, or bad things will happen".

e. Protected Health Information (PHI): Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. PHI includes but is not limited to all information protected under the Health Insurance Portability and Accountability Act. PHI does not include employment records held by a covered entity in its role as an employer.

f. Sensitive Information or Data: Any information that may only be accessed by authorized personnel. It includes Protected Health Information, financial information, personnel data, and any information that is deemed confidential or that would negatively affect the ADVA if inappropriately handled

g. Email: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.

13. **Federal VA computer users** must comply with Federal guidelines.

14. **Contacts:** For questions regarding the requirements, implementation, and enforcement of this standard, contact your supervisor or the ADVA Human Resources Manager in Little Rock, Arkansas @ 501-683-1386.

15. **Enforcement:** Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction. In addition, ADVA may report the matter to civil and criminal authorities as may be required by law.

16. **Forms Prescribed**: Employee Acknowledgement of ADVA Internet, E-Mail and General Computer Usage Policy.

BY:

Matt Snead
Director

Distribution:
A