

## **INFORMATION TECHNOLOGY SERVICES**

### **POLICY:**

It is the policy of ADEC to establish and maintain minimum requirements which, to the best of its knowledge and awareness, protect ADEC's information technology services (computers, local and wide area networks and attached computer servers, workstations and mobile devices) and the information assets they contain.

For all ADEC owned assets, including cellphones, computers and other electronic devices, reserved the right to audit and review content to ensure compliance with policy.

Willfully or neglectfully violating this policy may lead to disciplinary action including termination of employment.

Originator: Information Technology Services Manager

Latest Rev: 04/10/2023

Approved:

**PURPOSE:**

To establish requirements for the protection of ADEC's information technology services such as computers, local and wide area networks and attached computer servers, workstations and mobile devices; and the information assets they contain. In addition, to explain the privileges, responsibilities and risks of using the Internet, network resources and electronic mail (e-mail).

The policies and guidelines set forth in this document are neither voluntary nor optional. They are designed to protect ADEC, its resources and its personnel from the very real risks created by using ADEC's technology systems and the Internet. Violation of these policies and guidelines is grounds for disciplinary action up to, and including, dismissal.

These policies are intended to supplement, not replace, other ADEC policies. If you find a conflict among ADEC's various policies, please bring it to the attention of your manager.

Security exposures and Internet use continues to grow and evolve over time. These policies and guidelines are subject to change to reflect these new developments.

**10.1 AUTHORIZED USERS**

Every employee of ADEC is provided the technology tools necessary and appropriate to their jobs. The assignment of computers and related equipment to personnel is determined by an assessment of user need conducted by the Information Technology Services Department and recommendation by the appropriate Vice President. All recommendations may be subject to review by the President / CEO for final determination.

As a business tool provided by ADEC to its employees, it is expected that the use of all computer, mobile devices and related assets be restricted to legitimate business uses. All content on company devices is the property of ADEC.

**10.2 ELECTRONIC MAIL (e-mail)****10.2.1 Introduction**

E-mail is a quick and convenient way of communicating with others both inside and outside ADEC. The policies and guidelines set forth below are intended to protect both the sender and recipient of e-mail messages, as well as ADEC, from the pitfalls and risks that accompany use of e-mail. Unless otherwise noted, these policies apply to both internal ADEC e-mail and e-mail sent over the Internet. While these policies and guidelines specifically address e-mail, it is important to keep in mind that e-mail is just another form of business communication and is therefore subject to all ADEC policies, guidelines and practices relating to business communication in general.

**10.2.2 Internet e-mail security**

Internet e-mail is not a secure medium of communication. Internet e-mail can be easily intercepted and read by others. When sending Electronic Protected Health Information (e-PHI) outside of the ADEC network, the file

must be encrypted. Contact the Information Technology Services Department for additional information about encryption methods.

### 10.2.3 Monitoring of E-mail

You should use e-mail for agency purposes only, and not use e-mail or the Internet for any personal communications. E-mail messages sent or received by ADEC computer system via the Internet are not private. Best efforts will be taken to ensure that ADEC's internal e-mail system is secure from unauthorized access. Under this E-mail Policy, your usage of e-mail via ADEC technology is made with your consent that all e-mail communication at ADEC may be monitored by ADEC.

### 10.2.4 General E-mail Etiquette

E-mail is a useful business tool, however it can be abused in various ways. Familiarizing yourself with the following e-mail etiquette:

- Do not overuse e-mail by sending courtesy copies of a message to people who do not need them.
- Use distribution lists judiciously. When in doubt, consider checking the names of all users on distribution list before using it. Caution up front is the best way to ensure that your message reaches all the right people, and only the right people. Some agency and program-wide distribution lists require authorization to send to the list.
- Use discretion when forwarding e-mail messages. Use common sense: if you would not have forwarded a copy of a paper memo with the same information, do not forward the e-mail.
- E-mail is for business communication, not for advertising. Sending e-mail messages advertising personal activities such as garage sales or fund-raisers is inappropriate.
- E-mail is far more permanent than speaking to someone over the phone.
- E-mail does not convey emotion well. Use another method of communication when appropriate.
- When replying to e-mail, it is often useful to include a portion of the original sender's message to put your reply in context. However, it is also appropriate to delete unimportant portions of the original message in order to prevent the message from getting too long.
- Use normal capitalization and punctuation. Typing a message in all capital letters is the e-mail equivalent of shouting at the reader. You can, however, use capital letters to create emphasis. Prior to sending a message, it is recommended that you use spell check whenever possible.
- E-mail chain letters and other non-business related messages, i.e. solicitations, calls for action, jokes, etc., are inappropriate business use of the computer. Do not initiate or participate in such correspondence.
- Viruses are a high risk and sometimes sent as attachments to e-mail. As a precaution, do not automatically open e-mail attachments when you receive them from the Internet. If you do not know the person sending the e-mail, do not open attached documents, close the e-mail and delete it. Please contact the ADEC Information Technology Services Department if you have questions about e-mail or attachments.
- Phishing. Think of Phishing as someone actually fishing for your information or credentials. The bait used is an enticing e-mail that will attempt to trick you into doing something you would not normally do. The from address could be from someone you know and correspond with on a regular basis, but if it looks out of character or odd, then call that person to confirm they sent it or check with the Information Technology Services Department.
- Phishing e-mail. Please stay aware of e-mails you are receiving and if the e-mail is suspicious, please do not click on any links or attachments in the e-mail. If any link from an e-mail sends you to a sign-in page then it is probably a Phishing site made to look like an Office 365 or other sign in page. If you are unsure please verify with the Information Technology Services Department.

## 10.3 INTERNET

### 10.3.1 Use of the Internet

As with telephones, photocopiers, fax machines, and other technology supplied by ADEC, use of the Internet must be conducted in compliance with ADEC policies. Abuse of the Internet, or violation of ADEC policies and guidelines, is grounds for disciplinary action.

### 10.3.2 Internet Usage Guidelines

ADEC provides Internet access as a key resource to meet the information needs of individuals, the agency and our individuals served. We encourage the business use of the Internet to further our efficiency and our capabilities. However, the use of the Internet can be associated with business risks. It is ADEC's expectation that each user will be personally accountable for his or her appropriate use of the Internet. The following guidelines and information have been developed to help people make thoughtful decisions when using the Internet.

- Users should be aware that ADEC has the capability to monitor and record all Internet usage, e-mail message, and each file transfer into and out of our internal networks. ADEC reserves the right to do so at any time.
- Downloading and displaying or disseminating materials which may be considered by some people to be obscene, racist, sexist, defamatory or otherwise offensive, or which invades another person's privacy, may constitute harassment by creating a hostile work environment. Such actions are expressly forbidden. Moreover, they may subject both the offending employee and ADEC to legal action. ADEC is committed to maintaining a work environment free of any conduct that may be considered harassment. Violation of this policy is grounds for disciplinary action up to, and including, discharge.
- No person may use ADEC Internet facilities and computing resources to knowingly download or distribute pirated software or data. All software must comply with all laws and regulations regarding licenses or copyrights.
- ADEC Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States, or the laws and regulations of the state, city or other local jurisdiction in any way.
- ADEC's Internet facilities cannot be used to deliberately propagate any virus or malware. In addition, ADEC's Internet facilities cannot be used knowingly to disable or overload any computer system or network, or circumvent any system intended to protect the privacy or security of another user.

## 10.4 INFORMATION ASSETS

### 10.4.1 Introduction

Information assets include word processing documents, spreadsheets, databases and other information stored on the ADEC computer system. This includes any data that is also associated with enterprise-wide software tools including but not limited to MITC, ADP, Solana, Accuflo, Advocacy Links, BDDS portal, etc.

### 10.4.2 Security and Backups

ADEC network computers include subdirectories that limit access to individual users, as well as subdirectories that are shared between various users. The Information Technology Services Department is responsible for setting up appropriate security. It is the responsibility of the user to understand the different security options and become aware of the security settings of their stored documents.

ADEC networks are backed up daily. If a computer user chooses to store their data on an encrypted computer workstation when storing data on a network is not possible, it is the responsibility of the user to conduct regular backups of the data.

#### 10.4.3 Monitoring Information

Best efforts will be taken to ensure that information stored on ADEC network computers will be secure from unauthorized access. Under this policy, your usage of the ADEC technology is made with your consent to monitoring by ADEC. Use the technology appropriately. Do not use ADEC computers for communications that would embarrass you if reviewed by management, or which, for any reason, you would prefer to keep private.

#### 10.4.4 Software License Agreements

An employee must get approval from the Information Technology Services Department before installing software on an ADEC computer. All software must be in compliance with the Software License Agreement. Any software purchased by ADEC cannot be copied to a computer that is not owned by ADEC. Unauthorized copying of software will result in disciplinary action.

#### 10.4.5 Passwords

Passwords are the User's responsibility and may not be shared, unless expressly authorized by ADEC. Users will be able to select and change their passwords. It is required that passwords be changed annually. Permanent passwords are not permitted. Passwords must be at least eight characters long, and some software systems require 12 characters. Passwords **SHOULD** be a mixture of uppercase, lowercase, numbers and special characters. Password entry is case sensitive. Users should not write down passwords, store them on hardcopy or store them locally on workstations and laptop computers.

A good password practice is to use the first letter of a phrase. For example, the phrase "I work in Bristol Building 2 for \$" would look like IwiBrBu2for\$. It is recommended that users choose a unique password for ADEC sites, and not use the same password as non ADEC sites (example social media password).

Passwords include network passwords, Microsoft Windows passwords, startup passwords, inactivity time-out password, file password protection. In addition, Users are responsible to change the passwords to access specific software (example ADP, Blackbaud, Sandata, MyMITC for the Web).

Use unique passwords for ADEC systems. Do not use your ADEC password for systems outside of ADEC (for example Amazon accounts or personal e-mail accounts). Select passwords that are only used at ADEC. When setting up electronic access to work related sites (example Indiana State Websites, Disability or Vendor related sites) use a password other than your ADEC password. This will decrease the possible breach of your ADEC e-mail and network password. Use of password management software or password management App must be approved by the Information Technology Services Department.

#### 10.4.6 Multifactor Authentication

Multifactor Authentication. ADEC will utilize Multifactor Authentication where technically feasible. This includes Microsoft Office 365 and other remote access systems. Multifactor Authentication will require the ADEC employee to authenticate a second time using a phone or other device to confirm their identity and grant access to use the system. For Office 365 an employee will setup the initial Multifactor Authentication using the phone number of their primary ADEC work location, additional optional Multifactor Authentication can be setup and used with a personal cell phone.

#### 10.4.7 Electronic Protected Health Information (e-PHI)

It is expected that Staff will adhere to ADEC policies which protect the confidentiality of Protected Health Information and will not save Electronic Protected Health Information on a non-secure location or a non ADEC owned computer or mobile devices.

Employees will be familiar with workstation security requirements when accessing e-PHI. This includes use and change of passwords, limiting others from viewing ePHI on the workstation, securing mobile devices, and using inactivity timeouts and passwords. Employees will be familiar with workstation and mobile device Inactivity time-out settings. All computers and mobile devices that access e-PHI must have inactivity time-outs set to 15 minutes or less, where technically feasible.

The use of portable devices such as USB Flash Drives or USB Storage Devices used to store and transport e-PHI must be approved by the Information Technology Services Department. Additional records of e-PHI location will be maintained by the Employee and the Information Technology Services Department.

If you need to send Electronic Protected Health Information out of the ADEC network via email you will need to use encryption. Contact the Information Technology Services Department for more information on the latest encryption methods.

Employees should follow the established procedure for release of information. This includes information that employees post on social media (Face Book, Twitter, email, etc.). Such information should not include information about individuals served, including photos.

### 10.5 Personal Mobile Devices

ADEC employees who are issued an ADEC mobile device should use the ADEC mobile devices for business use and their personal mobile devices for personal use.

ADEC e-mail messages and ADEC Information Assets containing Electronic Protected Health Information should not be forwarded to personal mobile devices. Employees are not to download and store Electronic Protected Health Information on a non ADEC computer or personal portable devices. Individuals served photo and video are considered Electronic Protected Health Information; do not use your personal mobile device to take individuals served photos or videos.

For staff convenience and efficiency, ADEC allows for the use of employee personal devices to connect via a secure connection. Currently, this is limited to an employee connecting to the ADEC e-mail system to view e-mail, MyMITC for the Web, and ADP Employee Portal. For ADEC e-mail, employees are to only use the web version of Office 365 (Microsoft Online) and not install an App (for example the Microsoft Outlook App) on their personal device that downloads the ADEC e-mail. This avoids the possibility of an installed App allowing confidential company data to remain on an employee's phone. Use of the Microsoft Outlook App will be accepted for those eligible for policy 3.1.4.

ADEC employees are not to use their personal email or social media during their work hours as a source of information (example art, crafts, or recipes). There are legitimate sources for this information that does not involve compromising personal information and accounts during ADEC work hours.

## 10.6 iPad Controls

The following Controls for iPad and iPad Apps apply to other similar devices such as Android Tablets and Fire Tablets.

iPads are being used at ADEC for Assistive Technology purposes and are used with individuals served in Therapies and other programs. The iPads are not connected to the ADEC Enterprise Systems. The roles of Information Technology Services Department (IT) and Community Outreach related to iPad and iPad Apps are listed below.

### 10.6.1 Inventory List

- IT must be made aware of all iPad acquisitions and disposals.
- An iPad inventory list will be maintained by IT.
- iPad inventory list will be emailed at least annually to the CEO and CFO and kept by the IT department.

### 10.6.2 New Purchased iPads

- New purchase of iPad and related accessories will be handled by IT.
- The IT Department will complete all setup of the iPad including initial setup and security.

### 10.6.3 Donated iPads

- The donation of iPad and accessories will be coordinated by the Community Outreach Team who will communicate donated iPad information to IT.
- Donated iPads will be "wiped", going through an official Apple check list.

### 10.6.4 iPad Use

- Before ANY new iPads are put out to the field in Day Services, they will be given to the IT Department to be documented on the iPad inventory list, labeled for asset protection, and added to the appropriate control software, ensuring security and protection of all clients, staff and ADEC as a whole. The IT Department will document:



- Where they will be assigned, whom they are being assigned to and what they will be used for.
  - Individuals served will be encouraged to use iPads as part of their program goals or daily activities.
- IT will be informed if the iPad location or user changes.
- iPads cannot be connected to ADEC's servers.

#### 10.6.5 iPad Apps

The IT Department will:

- be responsible for purchasing, installing, and setting up iPad Apps.
- Approve all iPad Apps loaded on the iPad.
- iPad App purchases and iPad accessory purchases; this includes monitoring and approving any Credit Card purchases connected to the iPad.
- Establish controls on what Apps can be downloaded and who has specific access to sign-on and passwords. Such sign-on and password access must be very limited.
- Provide timely receipts for any iPad Apps or accessories purchased to Accounts Payable soon after the receipt of the goods.

#### 10.6.6 Repair

- IT may assist with iPad repair as needed; assisting as needed to diagnose hardware repair issues and to coordinate the iPad repair.



## ACKNOWLEDGEMENT AND CONSENT

By my signature below, I acknowledge that I have received a copy of the ADEC Information Technology Services Policy. I have read and understand the terms of the policy. I hereby consent to be governed by all terms as set forth in the policy.

Signed: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_