Fresno Regional Workforce Development Board

A proud member of America's Job Center of California[SM] Network

2125 Kern Street, Suite 208 • Fresno, California 93721 • 559.490-7100 • Fax 559.490.7199 • www.frwdb.net

Blake Konczal,

Executive Director

POLICY BULLETIN

FRWDB PB # 05-06, Revision B **Date Released: January 28, 2020**

To: All Fresno Regional Workforce Development Board Providers of Services

From: Blake Konczal, Executive Director

Effective Date: January 28, 2020

Subject: Information Technology Standards Policy

Applicable Program: All

Revision History: Initial Release – 4/20/06

This Revision B updates terminology for WIOA.

The Fresno County Workforce Investment Board (FCWIB), now known as the Fresno Regional Workforce Development Board (FRWDB) initially approved the Information Technology (IT) Standards and Replacement Policy at its meeting held on April 20, 2006.

The purpose of the policy is to ensure consistency in the procurement and utilization of FRWDB IT equipment and technology.

The Policy begins on page 2.

Any questions are to be addressed to the FRWDB Deputy Director of Information Services.

Fresno Regional Workforce Development Board
INFORMATION TECHNOLOGY POLICY

MISSION:

"To oversee the design and implementation of a seamless information system which meets the needs of partners and the reporting requirements for the purpose of supporting missions of the Fresno Regional Workforce Development Board."

GENERAL:

The Fresno Regional Workforce Development Board (FRWDB) and all entities receiving funding from the FRWDB will adhere to these policies and standards. Further, all entities will abide with all local, state, and federal laws pertaining to information technology licensing, copyrights, trademarks, and usage.

PURPOSE:

The purpose for defining policies and standards is to ensure maximum compatibility and integration between organizations, leading to efficient electronic interaction among contractors and partner agencies. Maintaining standards will provide a consistent and solid framework for expanding the electronic technology system within the Local Workforce Investment Area (LWIA) and, eventually, to neighboring LWIAs. Additionally, the maintenance of standards will provide for a more stable environment by making technology easier to manage and more reliable. Resources across the system can be leveraged more easily, thereby increasing the availability and effectiveness of technology.

An effective replacement policy will: 1) maximize availability, reliability, and application productivity for the end-user, 2) ensure technology is current in critical areas, 3) maximize productivity for technology support staff, 4) follow established FRWDB Procurement Policies, and 5) meet the standards for reasonableness and necessity. Attention to each of these areas produces a technology infrastructure that supports, rather than hinders, current activities and allows for more successful implementation of operational plans. Additionally, a sound technology infrastructure paves the way for innovation within the system by removing potential technological barriers, i.e. insufficient resources available to assess potential applications and technologies.

The end result is a continually improving system that is proactive in meeting the needs of our customers.

SCOPE:

The scope of this policy reflects the intent of the Fresno Regional Workforce Development Board (FRWDB) as it pertains to technology within the LWIA. This policy addresses the technology used by contractors for the purpose of completing the requirements of their contract for services with the FRWDB, and for technology procured in part or in whole with funds administered by the FRWDB or the Fresno Area Workforce Investment Corporation (FAWIC). However, it is recognized that the effectiveness of this policy is enhanced by participation from non-FRWDB funded organizations and, therefore, may be subject to modification to accommodate such participation. Further, specific reference to "brand name" products is not an endorsement of those products nor is it intended to circumvent the established procurement policy with respect to new or replacement purchases.

Technology not specifically addressed within this policy is not subject to the standards and replacement policy. However, with the approval of the FRWDB, the Executive Director of the FRWDB has final authority over all technology procured in part or in whole with Workforce Innovation and Opportunity Act (WIOA) funds.

CONFIDENTIALITY:

All WIOA-funded technology systems and users within the LWIA will assure the highest degree of confidentiality with respect to information input and/or stored in databases utilized by the system. There will be no exchange or divulgence of participant information to non-WIOA funded entities without first obtaining written approval from the participant. Likewise, the programs utilized by the system will not be compromised by disclosure to unauthorized parties. In all cases, information regarding or residing in the system will only be available to others on a pre-authorized, need to know basis.

SYSTEM SECURITY:

All systems utilized within the information technology infrastructure for the LWIA will be configured to provide for the highest degree of security from external system access. Internal users will have access to hardware, databases, and programs only to the extent required in the performance of their respective job duties and responsibilities.

INFORMATION TECHNOLOGY DEFINITIONS

The definitions presented are to identify the scope of technology to which this and all other technology policies and procedures apply. As new technologies are developed, the definition is to be updated by appropriate staff.

Technology is defined as any component that facilitates the electronic flow of information which includes, but is not limited to, computers, hardware, software, telephone systems, networks, copiers, printers, facsimile machines, video equipment, recorders, projectors, digital cameras, and support services.

- Computers include personal computers, hand-held devices, workstations, portable or mobile computers, servers, mainframes, or supercomputers.

- Hardware includes physical components and peripherals of computers or other electronic devices.

- Networks include networking equipment used to physically connect and secure computers, hardware, copiers, printers, and any other technology to any local or wide area network within the scope of this policy.

- Software is a collection of programs that control computers and hardware or processes data for computer or hardware users. These programs include system software and application software.

- Telephone systems include digital, analog, and cellular equipment used to facilitate voice communications.

- Copiers, scanners, and printers are those devices that reproduce electronic images and documents.

    - Copiers are either stand-alone or connected to network or computer equipment by a physical or wireless connection.
    - Printers and scanners are connected to network or computer equipment by a physical or wireless connection.

- Facsimile machines reproduce and transmit images or documents and are connected to internal or external telephone systems and network or computer equipment.

- Video equipment includes hardware and computer equipment used to capture, retrieve, or transmit digital or analog, still, or moving images. This includes recorders, projectors, and digital cameras connected to network or computer equipment, or stand-alone devices.

- Support services include technology services provided by external or internal human resources in the form of knowledge transfer or physical tasks. Examples include training, computer programming, system analysis, system administration, hardware troubleshooting and repair, etc.

STANDARDS

The technologies for which standards are to be maintained are as follows:

- Software
  - Operating systems
  - Mail applications
  - Office suite productivity tools
  - Document development
  - Anti-virus software
  - File compression
  - Internet browser
- Computers
  - Servers
  - Workstations
  - Notebooks
- Hardware
  - Uninterruptible Power Supplies (UPS)
- Networks
  - Physical wiring
  - Switches
  - Routers
  - Wireless
- Printers & Scanners
- Support Services
  - Training

Software

All software should be of a version that is necessary to the conduct of business and does not impede the speed or efficiency of the user. Technical staff are to monitor and maintain service packs, updates, etc. while ensuring ramifications are fully understood before installing.

- *Operating Systems* – Operating systems for all computers will be of the Microsoft Windows family, UNIX-based, and/or the Palm operating system.

- *Mail Applications* – Mail servers will run Microsoft Exchange, and Microsoft Outlook will be the mail client at the end-user's network workstation. Exceptions are those devices that by nature do not utilize Outlook; i.e. Palm OS.

- *Office Suite Productivity Tools* – The Microsoft Office family of office suite productivity tools shall be used. If the full suite is not required, the individual component will be used; i.e. if one desires a word processor application, Microsoft Word shall be used. Exceptions are: web development tools, desktop publishing tools, and image tools.

- *Document Development* – Adobe Acrobat and the PDF format will be used for publishing formal documents for electronic distribution outside of any organization. Exceptions are documents that require specialized functions such as formulas or if a document emanates from outside the Fresno LWIA and it is not efficient or possible to reformat the document. Desktop publishing shall be done with Adobe products.

- *Anti-virus software* – All computers will have anti-virus software that runs in memory and continuously monitors incoming and outgoing files and e-mail attachments. Virus signature updates shall be installed automatically per a schedule or as soon as possible after notification. In a networked environment, a network version of anti-virus software will be used.

- *File-compression* – WinZip will be used to compress files with the exception of UNIX compression tools within the UNIX environment.

- *Internet Browser* – Internet Explorer will be used. Appropriate plug-ins may be installed as needed for business use.

Computers

All computers will utilize the current generation of Intel Pentium processors unless another processor serves the greater benefit of the LWIA. When developing specifications for new computers, cost trades-offs should be maximized with memory having a high priority. The user's needs should always be considered when configuring a computer; ensuring resources are sufficient without being wasteful. For this purpose, configurations should be reasonable and necessary.

- *Servers* – Servers utilizing the Windows operating system shall be consistent throughout the organization maintaining the server environment. All servers will be from the same manufacturer until such time as it is determined that the manufacturer's quality of product and support is not sufficient to maintain efficiencies, is outdated, and/or has deteriorated as compared to other server systems. Documentation to support changing server manufacturers must be reviewed and approved by the FRWDB Executive Director. For organizations that have not procured servers at the time this policy is implemented, server procurements will be from the manufacturer in use at the FRWDB. When multiple servers are needed, a rack configuration within a temperature controlled, secured environment shall be maintained.

  Unix-based servers will be manufactured by Sun Microsystems to leverage existing UNIX administration skills and peer support from other LWIAs, and to ensure consistent quality and the broadest availability of third-party products.

- *Workstations* – Whenever possible, workstations will be obtained in quantities. Workstation manufacturers will be the same throughout the LWIA. All workstations will be from the same manufacturer until such time as it is determined that the manufacturer's quality of product and support is not sufficient or has deteriorated as compared to previous experience. For organizations not meeting this standard at the time this policy is implemented, all future workstations purchased will comply unless prior approval is obtained from the FRWDB Executive Director.

- *Notebooks* - Notebook manufacturers will be the same throughout the LWIA. All notebooks will be from the same manufacturer until such time as it is determined that manufacturer's quality of product and support is not sufficient to maintain efficiency, is outdated and/or has deteriorated as compared to other notebook equipment. Documentation for review by the Executive Director that supports changing notebook manufacturers must be maintained and available when requesting a change. For organizations not meeting this standard at the time this policy is implemented, all future notebooks purchased will comply.

- *Hand-held devices* – Palm or Hewlett Packard Jornadas may be used as personal information managers.

Hardware

- *Uninterruptible Power Supplies (UPS)* – APC UPSs are to be used as battery backup for all equipment that does not contain one in its design. Whenever possible, the UPS should be available for monitoring via the network and have the capability to notify the administrator in the event power is lost.

Networks

- *Physical wiring* - Wiring for data or voice shall be the latest category of standardized unshielded twisted pair (UTP).
- *Switches* - Switches are to be used whenever cost effective in place of network hubs. The switch shall have 100Mbs capability.
- *Routers* - Routers shall be manufactured by Cisco Systems
- *Wireless* - Wired access points and interface cards shall adhere to the 802.11b protocol.

Printers & Scanners

- *Printers* – All black and white printers shall be manufactured by Hewlett Packard. The model selected should meet the users' needs, ensuring resources are sufficient without being wasteful. Since color-printing technology is rapidly evolving, the selection of a color printer should only occur after assessing the current models available by multiple manufacturers.
- *Scanners* – Scanners should be manufactured by Hewlett Packard, unless integrated into a networked copier.

Support Services

- *Training* – Specific technical training shall be administered by entities certified by the manufacturer of the particular subject, if such certification exists. Otherwise, the trainer should have a positive reputation within the information systems community and be able to provide well-known references, if local only.

REPLACEMENT

Software

Plans for replacing software will adhere to the standards described in this policy. New or updated versions shall be tested prior to deployment to more accurately plan, thus minimizing disruption to the end-user. In all instances, replacements must meet the procurement standards established by the FRWDB and must satisfy the standards for reasonableness and necessity.

Computers

- *Servers* - Servers are to be replaced when it can be demonstrated that the server cannot efficiently run its primary application and it cannot be upgraded to provide this ability.

- *Workstations* - Workstations are to be replaced no sooner than three years from the original date of purchase unless compelling reasons warrant replacement. Funding permitting, outdated and inefficient workstations should be replaced within the program year in which the three-year anniversary occurs.

- *Notebooks* - Notebooks are to be replaced no sooner than three years from the original date of purchase unless compelling reasons warrant replacement. Funding permitting, outdated and inefficient notebooks should be replaced within the program year in which the three-year anniversary occurs.

Other Technology

Other technology should be continually assessed to ensure it is consistent with the purpose of this policy. Other technology should be replaced when it can be demonstrated that newer technology will increase productivity, enhance efficiencies, is cost justified, is firmly established within the industry, and meets standards.

Application

All technology shall adhere to all standards described herein. In the case of exceptions, contradictions, excluded technology, or requests to waive the standard, clarity and/or approval by the FAWIC Director is required. If existing technology is not in compliance with this policy at the time of its implementation, these standards and policies will apply. However, the Director has the authority to require technology that is out of compliance with this policy to be replaced at the contractor's sole cost and expense, should the technology be determined critical to the efficient operation of the system.

The existence of any standard or replacement policy does not negate the requirement to follow applicable procurement policies. If a conflict exists between a standard and current procurement policies, the procurement policy shall prevail.

Non-Authorized Software Policy

All software to be used on computers that attach to the FCWIB network must be approved by the Information Technology (IT) Department. Prior to acquiring software, the end-user group must confer with the IT Department to ensure that the software is compatible with the FCWIB network and hardware.

PIRATED AND ILLEGAL SOFTWARE

Definition

Software piracy is the theft of software through illegal copying of genuine programs or through counterfeiting and distribution of imitation software products or unauthorized versions of software products. Software piracy also occurs when someone makes more copies than permitted, or when, for example, he or she borrows a copy of a program from someone else. One of the most prevalent types of software piracy is simple, unlicensed copying by individuals or businesses. In the case of volume licensees, it can take the form of underreporting the number of installations of the software made across an organization. Disk swapping among friends and associates outside of a business environment is also included in this category.

Agency Policy

The FCWIB adheres to all laws including local, state, and federal. It is illegal to participate in pirating software. The contractors of the FCWIB are also required to adhere to all local, state, and federal laws.

Penalty

Any staff that is determined to be participating in illegal activities will be referred to the appropriate authorities. Participating in copying, installing, or distribution of illegal software will be referred to Human Resources for appropriate action.

Peer to Peer File Sharing Programs

In the last few years, the technology world has seen a rapid deployment of what are known as Peer-to-Peer File Sharing programs such as Napster, Kazaa, Morpheus and others. These programs allow users to share files with other users around the world. Because this file sharing technique allows others into our system it creates a security risk for our confidential files. It is for this reason that these programs are prohibited in our system. If you have a question as to a specific program, please ask the Help Desk.

Statement of Compliance with Copyright Laws

It is the policy of the FCWIB that no employee or contractor may engage in any activity that violates federal, state, or local laws with respect to intellectual property rights; the terms of software license agreements; or FCWIB policies pertaining to computer software. For any computer software owned by or licensed to the FCWIB and computer systems or hardware owned or operated by the FCWIB:

1. *Must abide by all terms of the software license agreement.*
2. *Must be aware that ALL computer software is protected by copyright unless it is explicitly labeled as PUBLIC DOMAIN.*
3. *Must not copy software for any purpose outside those allowed in that particular software's license agreement.*
4. *Must not make software available for others to use or copy in violation of that software's license agreement.*
5. *Must not accept unlicensed software from any third party.*
6. *Must not install, nor direct others to install, illegal copies of computer software or unlicensed software onto any agency-owned or operated computer system.*

Violations of this policy will be referred to the appropriate FCWIB disciplinary channels and may result in disciplinary action up to and including termination of employment, in addition to remedies sought by the copyright holder. If the violation is discovered to have involved a partner agency employee, the activity will be reported to the designated manager of the partner agency.

NETWORK MONITORING

The technology department, at the direction of the administration, randomly monitors e-mail, web activity, and other network traffic.

ACCEPTABLE USE POLICIES

E-Mail

The FRWDB provides e-mail accounts to all staff. Acceptable use of the e-mail system is defined as follows:

E-mail is to be used for employment-related activities. Since e-mail has an inherently personal nature, it is acceptable for staff and employees to use the e-mail system for personal correspondence on a minimal and incidental basis. In situations where e-mail is being used excessively for personal communications, the information will be turned over to the respective agency's Human Resources Department for action.

E-Mail Guidelines

1. It is unacceptable to use e-mail to conduct personal business not associated with your primary employment.
2. All e-mail is the property of the FRWDB. It is subject to monitoring at any time.
3. Never assume your e-mail messages are private or that only you or the recipient can read them.
4. Never send something that you would mind seeing on the evening news.
5. Never send chain letters through the Internet. Sending them can cause the loss of your Internet access.
6. Be professional and careful what you say about others. E-mail is easily forwarded.
7. Never give your User ID or password to another person.
8. System administrators that need to access your account for maintenance or to correct problems will have full privileges to your account.

E-Mail User Responsibilities

The content and maintenance of a user's electronic mailbox is the user's responsibility:

1. Check e-mail daily and remain within your limited disk quota.
2. Delete unwanted messages immediately since they take up disk storage.
3. Keep messages remaining in your electronic mailbox to a minimum.
4. Mail messages can be downloaded or extracted to files then to disks for future reference.

ACCEPTABLE USE POLICIES – DEFINITIONS

Ownership of Internet-Related systems - Internet-related systems (including but not limited to: computer equipment; software and operating systems; network accounts providing electronic mail, World Wide Web browsing, File Transfer Protocol, etc.; networking and intranet systems and software) are the property of the agency. They are to be used for business purposes in serving the interests of the company and of our clients and in the course of normal operations.

Monitoring - The company reserves the right to monitor all employee usage to ensure proper working order, appropriate use by employees, the security of company data, and to retrieve the contents of any employee communication in these systems. Management may access user files, including archived material of present and former employees without the user's consent for any purpose related to maintaining the integrity of the network, or the rights of the FRWDB or other users or for any other reasonable purpose.

Personal use - Personal use of the systems is authorized within reasonable limits as long as it does not interfere with or conflict with business use. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Employees should be guided by departmental policies on personal telephone use and, in case of doubt, should consult their supervisor or manager.

Archiving and backup of systems - All staff work product and e-mail is backed up automatically to a dedicated server on a daily basis. This is an important function designed to maintain records of communications and activity which replaces (or supplements) maintaining files containing memoranda, correspondence, etc. It will also help reconstruct your data files if your system crashes.

Acceptable Web Use

With the understanding that the Internet is a large information repository, and it is becoming a part of our everyday life, we understand that there will be personal use of the Internet. It is not the intent of this document to prohibit that use; it is the intent of this document to provide a format for that use. With that in mind, the following guidelines are established with regard to Internet usage.

Personal Use/Prohibited Activities

The following activities are prohibited at all times.

1. Unauthorized attempts to circumvent data security schemes; identify or exploit security vulnerabilities; or decrypt secure data are prohibited.
2. Attempting to monitor, read, copy, change, delete, or tamper with another employee's electronic communications, files, or software without the express authorization of the user (except for authorized Network Administration personnel) is prohibited.
3. Knowingly or recklessly running or installing (or causing another to run or install) a program (such as a "worm" or "virus") intended to damage or place an excessive load on a computer system or network is prohibited.
4. Forging the source of electronic communications, altering system data used to identify the source of messages, or otherwise obscuring the origination of communications is prohibited.
5. The use of Agency Internet-related systems to access, transmit, store, display, or request profane, racist, sexist or other offensive material (including messages, images, video, or sound) that violates the company's harassment policy or creates an intimidating or hostile work environment is prohibited.
6. Any use that is deemed to adversely affect the FRWDB is prohibited.

7. Any on-line statements about the FRWDB, its position on any issue or about any competitor are strictly prohibited, except those authorized by senior management and/or the legal department.
8. Users of Internet-related systems are further advised to consider that while they use agency systems, they represent the FRWDB just as they would at an agency function. Visits to web sites and other Internet use may reflect upon the FRWDB and should be undertaken in a serious, businesslike manner.
9. Web pages and links made available to the public must be approved by and developed in cooperation with Network Administration prior to activation.