

Information Technology Policies and Procedures

Table of Contents

I. Information Technology Office

- 1010 IT Office Mission and Purpose
- 1020 IT Office Staffing

II. Network Description

- 2010 Networking Standards
- 2020 Site Connectivity
- 2030 WIC Connectivity to DHS

III. Information Technology Usage

- 3010 Information Technology Resources
- 3020 Electronic File Storage
- 3030 Email
- 3040 Instant Messaging
- 3050 Internet
- 3060 Phone, Voicemail, Fax
- 3070 Cellular Phones
- 3080 Digital Imaging Systems
- 3090 Postage Machines

IV. Security

- 4010 Information Security
- 4020 Password Protection
- 4030 Virus Protection
- 4040 Email and Internet Security
- 4050 System Access
- 4060 Data Backup and Recovery

V. Computer Hardware

- 5010 Computer Hardware Standards
- 5020 Computer Hardware Installation and Maintenance
- 5030 Computer Hardware Disposal
- 5040 Non-Agency Computer Hardware

VI. Computer Software

- 6010 Computer Software Standards
- 6020 Computer Software Installation and Maintenance
- 6030 Non-Agency Computer Software

VII. Service and Support

- 7010 Service and Support Requests
- 7020 Service Providers
- 7030 IT Training
- 7040 IT Purchasing

POLICY NUMBER 1010: IT OFFICE MISSION AND PURPOSE

PURPOSE: To inform employees of the mission and purpose of the Information Technology Office.

POLICY: The IT Office operates under the guiding principles stated in its mission and vision statements, and towards the fulfillment of its established purpose and functions.

DEFINITIONS:

I. MISSION:

The mission of the Information Technology (IT) Office is to deliver high quality, focused and aggressive business solutions by offering program-centric services and cost-efficient communications and information technologies.

II. VISION:

The vision of the IT Office is to shape today's information to meet tomorrow's challenges.

III. PURPOSE:

The purpose of the IT office is to plan, design, develop and maintain the Agency's information technology infrastructure, in alignment with the Agency's strategic objectives. Functions include, but are not limited to, information technology planning and evaluation, purchasing, hardware and software installation, providing ongoing user support and training, implementing management standards and policies and procedures related to information technology processes, and providing for network and information security.

These standards, procedures, and processes may change as appropriate. The Agency reserves full discretion to add to, modify, or delete provisions of the Information Technology Policies and Procedures Manual at any time, in whole or in part, without advance notice, consent or approval.

POLICY NUMBER 1020: IT OFFICE STAFFING

PURPOSE: To inform employees of the composition of the IT Office and the primary responsibilities and functions of its staff.

POLICY: To assign IT Office staff appropriate levels of responsibility and job functions.

DEFINITIONS:

I. IT MANAGER

The IT Manager is responsible for providing leadership and direction for the Agency's information and telecommunication technology and has the overall responsibility for planning, designing, developing and maintaining the information infrastructure and telecommunications systems of the Agency.

II. NETWORK ADMINISTRATOR

The Network Administrator is responsible for the security, operation, and maintenance of all Agency's network systems and applications.

III. PC/NETWORK TECHNICIANS

PC/Network Technicians are responsible for hardware and software support, installation and configuration, cabling, and telecommunications support. They are the first level of help desk support.

POLICY NUMBER 2010: NETWORKING STANDARDS

PURPOSE: To describe the Agency's networking standards.

POLICY: The IT Office evaluates, adopts, and implements networking standards to create and maintain an efficient, cost-effective Local Area Network (LAN) that promotes the Agency's strategic initiatives.

PROCEDURES:

I. NETWORK ARCHITECTURE:

The Agency LAN employs a switched 10/100 Ethernet architecture at data transfer rates of 100 Mbps (10 Mbps for legacy devices, such as some printers). Devices on the network, such as computers, servers, printers, copiers, are arranged in a star topology, where all devices are connected to a network switch or hub. Protocols used for transmitting data include TCP/IP and Novell NetWare's IPX/SPX.

Network devices are connected with category 5/5e unshielded twisted pair cabling, fiber optic cables, or wirelessly using 802.11b/g specifications. Category 5/5e unshielded twisted pair cabling is the most widely used media to connect Agency network devices. Fiber optic cabling is used where distances exceed category 5/5e standards. It is employed at Executive Plaza, SOUL/Sanctuary, and Transit/Food Services. Wireless connections are used at SOUL and at Executive Plaza in the IT Training Room and for mobile network connections in other training and conference locations.

II. NETWORK HARDWARE:

The IT Office selects and installs the following network hardware:

- A. Switches:** HP ProCurve or DELL PowerConnect, various models
- B. Firewalls:** SonicWall, various models
- C. Routers:** Cisco, various models
- D. Servers:** DELL PowerEdge, various models. Legacy servers are HP NetServers, various models.

III. NETWORK OPERATING SYSTEMS:

The Agency employs Novell NetWare, Novell Open Enterprise Server, and Microsoft Windows Server network operating systems. Novell NetWare or Open Enterprise Server is installed on the Agency's primary file, print, mail, and web servers, and Novell's eDirectory is the Agency's primary object and user authentication and identity management directory. The Agency has nine Novell NetWare/Open Enterprise Server servers in production. Microsoft Windows Server 2000/2003 is installed on application servers utilizing Microsoft SQL Server 2000. The Agency has six Microsoft Windows servers running MS SQL database applications. These applications are Financial Edge (accounting), iVantage (Human Resources information system), ChildPlus (Head Start information system), PowerSchool (SOUL student information system), GE Centricity Practice Management (Health Services practice management), and VersaTrans (Transit routing and scheduling).

POLICY NUMBER 2020: SITE CONNECTIVITY

PURPOSE: To describe how Agency sites are connected to each other through the Agency's local area network (LAN). See Diagram 2.1 for a visual depiction of the Agency's site connectivity.

POLICY: The IT Office is committed to fostering communication and information sharing among Agency programs and staff through appropriate and cost-effective methods of connectivity to Agency network systems.

PROCEDURES: The IT Office recommends and installs various methods of connectivity between Agency sites, depending on the availability and cost of the type of connection, number of employees at the locations, and the type and amount of data required to be transmitted.

I. T-1 LEASED LINE

A. Description and Purpose: The IT Office installs T-1 leased lines to connect larger Agency sites with high bandwidth requirements to the main Agency site at Executive Plaza 1920 Mariposa Mall. A T-1 leased line is a telephone connection between two points set up by a telecommunications carrier and provides a maximum transmission speed of 1.544 Mbps. The connection is always active, does not use the Internet, and therefore the full bandwidth is available between the two sites. T-1 lines are used in locations containing network file servers, where remote access to Agency applications is required, and where there is a large number of employees.

B. Installation and Configuration: The IT Office orders T-1 leased lines from AT&T. AT&T will install the line to the minimum point of entry at each end (site) of the circuit. Either AT&T or a local telecommunications vendor can also extend the line to the desired location at each end, for example, to the phone/network room, and terminate it with a RJ-45 jack.

T-1 leased lines connect the following Agency sites:

1. SOUL/Sanctuary to Executive Plaza
2. Local Conservation Corps to Executive Plaza
3. Health Services to Executive Plaza
4. Food Services/Transit Systems to Executive Plaza

Each end of the T-1 line is connected to a Cisco router, which is then connected to a network switch. The four "remote" sites each have a Cisco 1720 router. Executive Plaza has a Cisco 2600 router to accommodate the four T-1 circuits. Through the Cisco routers, the remote sites are not only connected to Executive Plaza, but to each other as well. No firewall is necessary at the remote sites since Internet access goes through Executive Plaza.

II. DIGITAL SUBSCRIBER LINE (DSL)

A. Description and Purpose: The IT Office installs DSL lines at smaller Agency sites with three or more networked computers in order to connect that site to the Internet. DSL technology allows data to be transferred over existing copper telephone lines. DSL lines connect the site to the local telephone switching station and then out to the Internet, not directly to another Agency site. DSL lines can only be installed in locations that lie within approximately 20,000 feet of the central telephone office. Therefore, DSL technology is not available in all locations, especially in the rural areas. The IT Office installs ADSL (Asymmetric Digital Subscriber Line) lines, which offers bandwidth of 384 Kbps upstream, and up to 1.54 Mbps downstream. As the telephone company shares its available DSL bandwidth among all of its DSL customers, the actual bandwidth at DSL sites fluctuates. For this reason, DSL lines are generally used only for GroupWise email and Internet access, and remote desktop support.

B. Installation and Configuration: The IT Office orders DSL lines from the local telephone vendor. The local telephone vendor can install the circuit on a dedicated telephone line, or on an existing telephone line already used for voice/fax. If the DSL circuit is placed on an existing voice or fax line, a DSL filter must be installed on the voice/fax jack to separate the data from the voice. The IT Office prefers to install DSL on existing fax lines. The local telephone vendor will install the DSL jack at the desired location next to the network equipment.

DSL lines are installed at the following Agency sites:

1. Transitional Living Center 1
2. Transitional Living Center 3
3. SOUL Asian Village
4. Head Start Franklin
5. Head Start Kings Canyon
6. Head Start Area II
7. Head Start Funston
8. Head Start Molly Nevarez
9. Head Start Brooks
10. Head Start Garden Way
11. Head Start Homebase A/B
12. Head Start Dakota Circle
13. Head Start Roosevelt
14. Head Start Sanger
15. Head Start Jefferson
16. Head Start Yosemite
17. Head Start Maintenance
18. Sanger LIHEAP
19. Early Head Start EPU
20. Early Head Start Clovis
21. WIC First Street Clinic

The DSL line is connected from the DSL jack to a DSL modem provided by the local telephone vendor as part of the service purchase. The modem is in turn connected to a SonicWall firewall, purchased separately and installed by the IT Office. The firewall establishes a Virtual Private Network (VPN) connection to the Agency's LAN over the Internet, and protects the site's network from unauthorized outside access.

III. DIAL-UP

A. Description and Purpose: The IT Office installs dial-up connections at sites with 1-2 computers or where higher speed broadband connections are not available. A dial-up connection uses a computer modem attached to a dedicated analog telephone line, and makes a dial-up connection to a modem located at Executive Plaza. A dial-up connection provides the lowest transmission rate of the connection methods used at the Agency. The transmission rate fluctuates, depending on line condition/quality and any interference, but is usually between 20-

30 Kbps. Dial-up connections are used for GroupWise email and Internet access, including access to the California Liheap Automated Services System (CLASS).

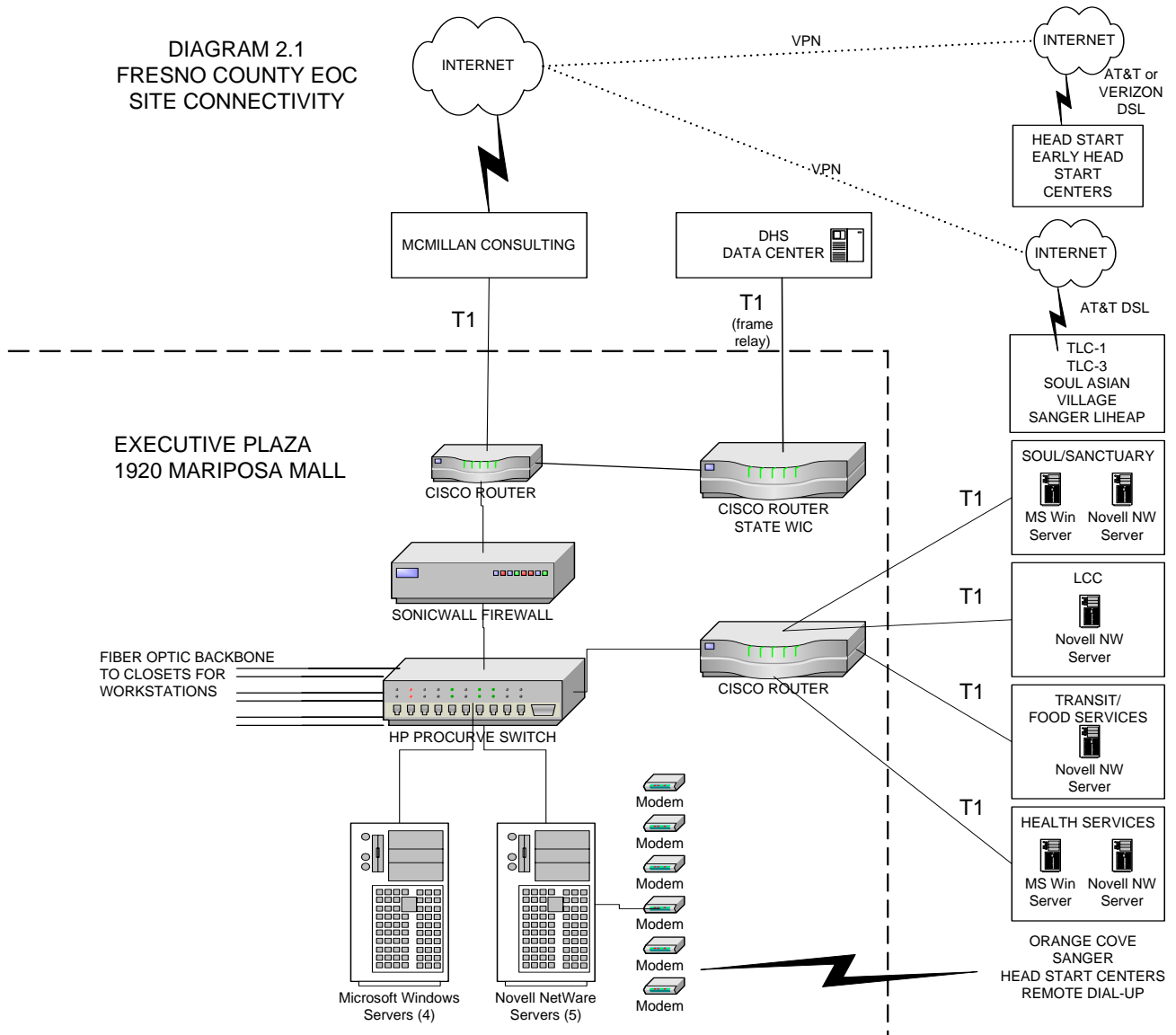
B. Installation and Configuration: The IT Office installs a modem in each computer that is designated for dial-up connectivity, and plugs in a dedicated analog phone line into the modem. If no dedicated analog line is available, the IT Office will arrange with the local telecommunications company to install a new line. If a dedicated line cannot be installed, the line may be shared between the modem and an existing voice/fax device. However, only one device can be used at a time. The IT Office configures a Windows dial-up connection on the computer, and issues a login ID and password to each staff member who will use a dial-up connection.

Dial-up connections have been established at the following EOC sites:

1. Orange Cove Community Services
2. 26 Head Start and HomeBase centers

To accept incoming dial-up connections, there are six modems attached to a Novell NetWare server located in Executive Plaza and running Novell Internet Access Server software. Each modem is connected to a dedicated phone line, and all lines are placed into a hunt group. Currently, six users can be simultaneously connected to the Agency's network using dial-up connections. Each session has a maximum connection time of 2 hours.

DIAGRAM 2.1
FRESNO COUNTY EOC
SITE CONNECTIVITY



POLICY NUMBER 2030: WIC CONNECTIVITY TO DHS

PURPOSE: To describe how the Women, Infants, and Children (WIC) program is connected to the State of California's Department of Health Services (DHS) Data Center, which lies outside of the Agency's LAN.

POLICY: The IT Office will comply with DHS mandates and ensure continued WIC program connectivity to the Data Center while maintaining the security of the Agency's LAN.

PROCEDURES: In order to access ISIS and WIC Extranet applications, WIC desktop devices, which reside on the Agency's LAN, connect to the Data Center through a T-1 frame relay line provided by the state of California.

I. DESKTOP DEVICES:

WIC management determines whether individual staff will have an Agency-standard desktop computer or a "thin client" to access applications at the Data Center. Both types of desktop devices reside on the Agency's LAN.

A. Desktop Computers: Agency standard desktop computers access the Data Center's ISIS application using locally installed IBM TN3270 emulation software, and access the WIC Extranet using Citrix client software and Internet Explorer browser. Desktop computers also have the ability to access the Agency's GroupWise email system, web browsing, and Microsoft Office applications.

B. Thin Clients: "Thin Client" computers are computers with little or no hard drive capacity and connect to remote servers, where all the data processing is done. The Agency standard thin client computer is the NeoWare thin client. Thin clients have built-in TN3270 emulation software to access the Data Center's ISIS application. Agency thin clients also access the state Immunization Registry via the Internet.

II. CONNECTIVITY TO DHS DATA CENTER:

The T-1 frame relay line to the Data Center is connected to a state-provided Cisco router located in the Agency's server room. The state router is connected to an Agency Cisco router located *outside* of the Agency's network firewall. The Agency's firewall and router allow/forward traffic to and from the Data center over the state-provided T-1 frame relay line.

III. RESPONSIBILITY:

A. Department of Health Services: The Department of Health Services is responsible for the functioning of the T-1 frame relay line and the state-provided network equipment. DHS is also responsible for establishing voucher printer names and ID's in the ISIS system. Any problems with these should be directed to the ISIS help desk at 800-224-7472.

B. IT Office: The IT Office is responsible for the functioning and configuration of Agency routers and firewall to ensure WIC staff connectivity to the Data Center. The IT Office is also responsible for desktop computer and thin client support, for voucher printer troubleshooting (along with WIC program staff), and for connecting desktop devices to the voucher printers.

POLICY NUMBER 3010: INFORMATION TECHNOLOGY RESOURCES

PURPOSE: To define Agency information technology resources and usage.

POLICY: Employees may access and utilize Agency-owned or administered information technology resources only as granted by the Agency and solely for the purposes of conducting Agency business and its related activities.

REFERENCE: FCEOC Personnel Policies and Procedures Manual, Policy 5100: Privacy and the Use of FCEOC Resources; FCEOC Employee Handbook, Workplace Practices: Information Technology Use

PROCEDURES:

I. DEFINITION:

Agency-owned or administered information technology resources include, but are not limited to, computer system hardware and software, network equipment, servers, software and services, email and instant messaging systems, telephone and voicemail equipment and services, video equipment, printers, scanners, and other imaging systems, fax machines, copiers, other electronic equipment, and all electronic files and storage media.

II. USAGE:

Access to and usage of Agency information technology resources is made available to employees at the sole discretion of the Agency and only for purposes of conducting Agency business and its related activities. Employees are prohibited from using Agency information technology resources to engage in behavior that would violate Agency policies, or local, state, or federal regulations. Employees should have no expectation of privacy, and, in fact, do not have privacy rights in the use of these resources, including email, voicemail, electronic files, and the Internet. Employees are expected to use Agency technology resources in a cooperative manner so as to make maximum use of the resources available. Use of Agency technology resources during non-business hours is prohibited unless permission is obtained from a Director or Assistant Executive Director.

POLICY NUMBER 3020: ELECTRONIC FILE STORAGE

PURPOSE: To establish guidelines for employees to follow regarding the storage of electronic files to meet business needs and also to maintain the health of Agency networks and servers.

POLICY: Employees are to store only work-related files onto Agency storage devices, in a manner that maximizes and does not jeopardize the use of available disk space, especially on network servers. The IT Office may periodically request employees to delete their unneeded files, and may delete without notice inappropriate files that are jeopardizing network or server functionality.

PROCEDURES:

I. TYPES OF FILES:

Employees may store files, with some restrictions and limitations, such as word processing documents, spreadsheets, presentations, databases, newsletters and flyers, digital photos, instructional video files, and other types of business documents. Employees may not store music files.

II. FILE STORAGE LOCATIONS:

Employees who log in to a network file server have a "home" folder and are encouraged to save their files into this folder. Files to be shared with other network users should be saved to "group" folders established by the IT Office upon program management request. Files saved to a network file server are backed up regularly and can be accessed from any network-connected computer, but only with the appropriate access rights.

Employees may also save to their computer's hard drive, but the IT Office does not back up the hard drives of employee computers. The files may be lost if the hard drive crashes. In addition, files stored onto a computer's hard drive are less secure than those stored on the network. Those employees who do not log in to a network file server and must save files to their computer may request to purchase external storage devices to back up their files, such as a CD-burner or a flash drive. The purchase and use of these devices must follow all Information Technology and Personnel Policies and Procedures. The IT Office does not promote or support the use of 3 ½" floppy disks to store Agency files. The IT Office will assist in transferring files from existing floppy disks to the network.

High-resolution digital photos should not be stored on the network for extended periods of time. They should be moved onto other storage devices such as CD-burner, external hard drive or flash drive for archival purposes.

III. FILE CLEANUP:

Network file servers are designed only to store files necessary for employees to conduct current business. Network file servers are not permanent repositories of all employee files. Employees are expected to regularly delete unneeded files from their "home" and "group" folders. The IT Office may enforce this policy by periodically requesting that employees delete unneeded files from the network. Employees may move needed files from the network onto other storage devices such as CD-ROM, external hard drive or flash drive if necessary and if proper authorization is obtained. The IT Office may delete inappropriate files from the network without notice if server or network health is in jeopardy, or to limit network disk space available to employees.

POLICY NUMBER 3030: EMAIL

PURPOSE: To establish standards and guidelines for employee email usage and to promote performance and stability of the Agency's email system.

POLICY: The Agency provides email accounts to appropriate employees in order to facilitate Agency business, in compliance with Agency policies and local, state, and federal regulations.

REFERENCE: FCEOC Personnel Policies and Procedures Manual, Policy 5100: Privacy and the Use of FCEOC Resources; FCEOC Employee Handbook, Workplace Practices: Information Technology Use

PROCEDURES:

I. EMAIL STANDARD:

The Agency uses Novell GroupWise as its standard email and collaboration software. Employees may not use other email systems or clients, including personal email or webmail accounts, on Agency technology resources. The standard internet email address for employees is firstname.lastname@fresnoeoc.org. Employees receive email accounts at the discretion and approval of their Assistant Executive Director or designee.

II. EMAIL USAGE:

Employees are to use Agency email for the purposes of conducting Agency business and work-related activities, and usage in violation of Agency policies or local, state, or federal regulations is prohibited. Examples of prohibited uses of email include, but are not limited to:

- Viewing, storing, soliciting, or forwarding pornographic images or other perceived obscene, racist, or harassing materials.
- Sending electronic mail that is non-business related, obscene, racist, harassing, jokes, violent or otherwise offensive.
- Solicitation, distribution or forwarding electronic games, music, video, or other non-business related materials.
- Solicitation, distribution or forwarding of non-work related information, such as requests for signatures, charitable contributions, support of political or organizational activities, or requests for donations.
- Bidding/purchasing of merchandise or services.
- Forwarding electronic chain letters.

To protect the Agency's email system, incoming file attachments larger than 8 megabytes are blocked. The incoming email message will come through, but with a notation that the attachment was blocked. Individual employee exceptions to this restriction must be approved by an Assistant Executive Director. Although there are no restrictions to the file size of outgoing email attachments, employees must exercise good judgment in the amount and size of any email attachments sent to others, including to other employees. Employees should recognize that other email systems may block the attachments they are sending.

For mobile and offsite email access, employees may access their GroupWise accounts from any Internet-connected computer or device via the web at <http://mail.fresnoeoc.org>. Employees must enter their username and GroupWise password at the login screen.

III. EMAIL RETENTION AND MAINTENANCE:

In order to maintain an efficient email system and to promote manageable individual employee email accounts, the IT Office runs a monthly purge of all GroupWise email accounts. This purge occurs on or about the first business day of every month, and will purge ALL email messages,

that are older than the preceding month. For example, a purge run on June 1 will delete all messages from before May 1. Email messages will be purged not only from the Mailbox, but also from any other location, including the Cabinet, Sent Items, Trash, Work In Progress, and all user-created folders. Calendar items are not purged. Employee exceptions to this policy must be approved by an Assistant Executive Director.

Recently deleted and purged email messages (within 15 days) *may* be retrievable by the IT Office from backup tapes. To prevent this issue, employees are encouraged to save email attachments and email messages outside of the email system to an appropriate storage device. Email messages can be saved as MS Word documents outside of the email system. Email archiving is not permitted except by approval of an Assistant Executive Director, as storing email messages in archive folders consumes more disk space than within the email account.

POLICY NUMBER 3040: INSTANT MESSAGING

PURPOSE: To establish standards and guidelines for employee use of instant messaging (IM).

POLICY: The Agency provides GroupWise Messenger as the standard instant messaging system to promote increased collaboration, communication and productivity. The download, installation, and use of any other IM system (Yahoo Messenger, MSN Messenger, AOL Instant Messenger, etc.) is prohibited.

REFERENCE: FCEOC Personnel Policies and Procedures Manual, Policy 5100: Privacy and the Use of FCEOC Resources; FCEOC Employee Handbook, Workplace Practices: Information Technology Use

PROCEDURES: GroupWise Messenger is available to all employees with network accounts. It is installed by the IT Office on all Agency computers assigned to employees. For security purposes, GroupWise Messenger can only be used within the Agency network; it cannot be used to send and receive instant messages with persons outside the Agency network.

Employees are to use GroupWise Messenger solely for Agency business purposes and work-related activities, and usage in violation of Agency policies or local, state, or federal regulations is prohibited. Examples of prohibited IM content include, but are not limited to: non-work related, obscene, racist, harassing, violent and/or otherwise offensive content. Even though IM is fast, easy, real-time communication, it is still business communication and must be treated as such. Employees are advised that as with email messages, IM conversations are not private. They can be saved as files and/or printed by participants, and are subject to Agency inspection and monitoring.

POLICY NUMBER 3050: INTERNET

PURPOSE: To establish standards and guidelines for employee use of the Internet

POLICY: The Agency provides Internet access to employees to facilitate communication, information sharing, research, resource development, and education. Use of the Internet for non-business purposes or in violation of Agency policies or local, state, or federal regulations is prohibited.

REFERENCE: FCEOC Personnel Policies and Procedures Manual, Policy 5100: Privacy and the Use of FCEOC Resources; FCEOC Employee Handbook, Workplace Practices: Information Technology Use

PROCEDURES:

I. METHOD OF ACCESS:

The IT Office implements various methods of Internet access, depending on the availability and cost of the type of connection, and number of employees at the locations. Programs located at Executive Plaza are connected to the Internet via a T-1 line to the Agency's Internet Service Provider (ISP), McMillan Consulting. Programs at SOUL/Sanctuary, Transit/Food Services, Health Services, and Local Conservation Corps all connect to the Internet through Executive Plaza via point to-point T-1 lines. TLC1, TLC3, SOUL Asian Village, and the larger Head Start and HomeBase Centers are connected to the Internet via Digital Subscriber Lines (DSL) from AT&T or Verizon. Dial-Up access to Executive Plaza then out to the Internet is provided to the smaller Head Start and HomeBase Centers, Sanger Partnerships, and Orange Cove Community Services.

II. APPROPRIATE USAGE:

The Agency provides Internet access solely for the purposes of conducting Agency business and related activities, and in compliance with Agency policies and local, state, and federal regulations. Prohibited Internet activities include:

- Viewing, storing, downloading or forwarding pornographic images or other perceived obscene, racist, or harassing materials.
- Sending electronic mail that is non-business related, obscene, racist, harassing, jokes, violent or otherwise offensive.
- Hacking, including attempting to gain access to restricted information.
- Downloading, distributing, or forwarding software, electronic games, music, video, or other non-business related materials.
- Participating in non-work related chat rooms or listening to Internet music.
- Solicitation, distribution, or forwarding of non-work related information, such as requests for signatures, charitable contributions, support of political or organizational activities, or requests for donations.
- Bidding/purchasing of merchandise or services.
- Downloading or forwarding chain letters.
- Gambling or any other illegal activity.
- Any other activities that violate Agency policies.

III. AGENCY RIGHTS:

The Agency reserves the right to monitor employee Internet activity, to block inappropriate web sites and content, and to limit access to employees at its discretion. Content filtering software is installed on all Agency firewalls to control access to inappropriate or objectionable web sites, but employees are still responsible for any access to inappropriate sites that are not blocked. Employees should notify the IT Office of any sites that are blocked that possibly

should not be. The IT Office will unblock these sites if they are obviously business-related. The IT Office may also block inappropriate sites that are missed by the content filtering software.

POLICY NUMBER 3060: PHONE, VOICEMAIL, FAX

PURPOSE: To describe IT Office and employee procedures and responsibilities for the use and support of Agency phone systems, voicemail systems, and fax devices.

POLICY: The IT Office is responsible for the purchase, installation, and support of Agency phone systems, voicemail systems, and fax devices. Employees have certain responsibilities and are expected to follow certain guidelines in the use of these resources.

REFERENCE: FCEOC Personnel Policies and Procedures Manual, Policy 5100: Privacy and the Use of FCEOC Resources; FCEOC Employee Handbook, Workplace Practices: Information Technology Use

PROCEDURES:

I. PHONE SYSTEMS:

The IT Office is responsible for the purchase, installation, and support of Agency phone systems. Service and support on Agency phone systems may be provided by IT Office staff, or by authorized third-party telecommunications companies. The appropriate program staff must advise the IT Office of any adds, moves, or changes, and the IT Office staff will either perform the work or contact the appropriate service and support entity.

Employees may not utilize third-party long distance companies to make long distance phone calls on Agency phone systems, and must refrain from utilizing "411" to call information. Both of these types of calls create an unnecessary expense to the individual programs. The Agency receives government pricing on long distance calling, and employees should utilize the online Fresno County yellow/white pages on the Agency Intranet at www2.fresnoeoc.org. The Agency reserves the right to limit the types of phone services available to employees, including long distance capability.

Only authorized Agency staff may make billing requests and place orders with the local telephone service provider (AT&T for most Agency locations, Verizon for Agency locations in Sanger, Reedley, Fowler, Cantua Creek, San Joaquin, and Firebaugh). Authorized employees are:

For Billing Inquires and Issues

Finance Director
Assistant Finance Director/Controller
Accounts Payable staff
IT Manager

To Place Orders

Executive Director
Assistant Executive Directors
IT Manager
Network Administrator
Head Start Education Director (Head Start/HomeBase Centers only)
Head Start Facilities and Maintenance Director (Head Start/HomeBase Centers only)
Approved third-party telecommunications companies

To Order Data Circuits

IT Manager
Network Administrator
Approved third-party telecommunications companies

II. VOICEMAIL SYSTEMS:

The IT Office is responsible for the purchase, installation, and support of Agency voicemail systems. Service and support on Agency voicemail systems may be provided by IT Office staff, or by authorized third-party telecommunications companies. The appropriate program staff must advise the IT Office of any adds, moves, or changes, and the IT Office will either perform the work or contact the appropriate service and support entity. However, under mutual understanding and agreement between the IT Office and individual programs, authorized program employees may perform their own voicemail box adds, moves, and changes on systems at locations other than Executive Plaza.

Employees who have voicemail boxes are required to add their mailbox into the voicemail system address book, and to record an appropriate standard greeting. Employees must also update the greeting when out on vacation, sick or other leaves of absence, traveling, or otherwise out of the office. Employees should forward their phones directly to voicemail when they are away from their desk. Employees must regularly check their voicemail, at least twice a day. Answering machines may not be installed on phone lines for employees that have access to a system voicemail box.

III. FAX DEVICES:

The IT Office is responsible for the purchase, installation, and support of Agency fax devices. The IT Office will work with Agency programs to obtain the appropriate fax device, whether it be a stand-alone fax machine, a multi-functional device, a fax module in a digital imaging system (copier), or other device. The IT Office strives to consolidate fax functionality into other devices to minimize the number of pieces of equipment, saving space, toner, and support costs. Appropriate employees should contact the IT Office when fax devices are not working properly, as it may be less expensive to purchase a new fax device than to service and repair a non-working device.

Employees are prohibited from using Agency phone, voicemail, and fax systems to engage in behavior that would violate Agency policies, including but not limited to communication containing racist content of any kind, sexual innuendoes, or any other inappropriate content. Employees are expected to limit the personal use of these systems to occasional and infrequent needs, without compromising their own work or disrupting other employees' work.

POLICY NUMBER 3070: CELLULAR PHONES

PURPOSE: To compensate authorized employees for business use of their personal cellular phones and to communicate guidelines and responsibilities for employee cellular phone usage for business purposes.

POLICY: The Agency will offer a stipend for cellular phone service to employees whose duties and responsibilities entail cellular wireless access to telephone and/or data service. Stipends will fall under a Low, Medium, High, or Other level of compensation.

DEFINITIONS:

Cellular phone service for the purposes of this policy is any service that is being used, in any measure, to make or receive wireless telephone calls or transmit data on the public cellular telephone networks.

A cellular phone (cell phone) for the purposes of this policy is any device that is capable of using the services provided by the public cellular telephone networks. These devices vary from a simple telephone device that allows calls to be made and received and perhaps provide simple features such as a phone number directory, simple appointment calendar, and calculator to more complex phones that can do simple text messaging and synchronizing directory and calendar data with computers, to devices with telephone features and PDA (personal digital assistant) capabilities which would include fully synchronized contact databases, calendars, email, and web browsing, to general computers with cellular phone network cards.

PROCEDURES:

I. ELIGIBILITY:

A monthly stipend would be issued to those employees whose duties entail the use of a cell phone. The appropriate Assistant Executive Director would determine the monthly stipend level for the employee, which would be one of the four levels of compensation: Low, Medium, High, or "Other."

The employee would be responsible for acquiring a cell phone account and cell phone, and would bear all costs for equipment and services. Most employees that would need to use a cell phone for business purposes already have a personal cell phone account. The cellular phone service falling under the Stipend Plan will not to be purchased by, licensed or directly billed to the Agency. The monthly stipend may be taxable income; therefore the individual may be taxed according to the regulations of the IRS code.

Only employees authorized by an Assistant Executive Director using established criteria may participate in the Cell Phone Stipend Program. Reasons for requiring an employee to have a cell phone are:

- Safety requirements indicate having cell phone service is an integral part of performing duties of the job description.
- More than 50% of work is conducted in the field.
- Employee is required to be contacted on a regular basis (no office).
- Employee is unavailable much of the time by any other means than cell phone
- Employee is required to be on-call outside of normal work hours.

- Employee is a critical decision-maker.

II. ENROLLMENT:

To enroll an employee in the Cell Phone Stipend Program, the following procedures must be followed:

1. A Cell Phone Authorization Request must be completed and signed by an Assistant Executive Director. The applicable criteria and desired stipend level must be checked. The following schedule may be used to help determine the appropriate stipend level:

Low: This stipend is for the employee who has light usage of the cellular phone for business purposes and would normally use up to 250 minutes per month.

Medium: This stipend is for the employee who has medium usage of the cellular phone for business purposes and would normally use from 250 to 499 minutes per month.

High: This stipend is for the employee who has heavy usage of the cellular phone for business purposes, or may frequently travel out of the local/regional area and would normally use more than 500 minutes per month.

Other: This stipend is for employees whose usage does not fit into one of the other stipend designations, or for a critical decision maker.

2. The employee must complete and sign the Cell Phone Stipend Program Agreement. The Agreement stipulates that the employee:
 - Will obtain, at their own expense, a cell phone and cell phone account from a cell phone service provider that provides effective cell phone service throughout the anticipated usage areas.
 - Will make their cell phone number known to their supervisor and other program staff as required.
 - Will carry their cell phone and have it turned on during their work hours (including on-call hours), and will use their cell phone as necessary to conduct Agency business.
 - Will not use their cell phone for business purposes while driving a vehicle unless they are using a hands-free accessory.
 - Will comply with the Cellular Phone Policy and all Agency policies and procedures.
3. The completed forms are to be submitted to the Human Resources Office, who will enroll the employee in the Stipend Program.
4. The stipend payment will be distributed as part of the employee's bi-weekly pay while the employee is part of this program.

The Human Resources Office will, on a quarterly basis or upon request, provide each Assistant Executive Director with a report of those employees in their programs who are participating in the Stipend Program. The Assistant Executive Director will review the report to determine if any employees no longer need cell phone service for business purposes. Additions, deletions, and stipend levels may be adjusted at any time by the written request of an Assistant Executive Director.

III. USAGE:

All costs related to the purchase and usage of the cellular phone service is the responsibility of the employee. Use of the phone in any manner contrary Agency policy or local, state, or federal laws will constitute misuse, and may result in immediate termination of the cell phone service stipend.

IV. TERMINATION:

If an employee is terminated, resigns, transfers or no longer eligible for a cellular phone service stipend, the Human Resources Office will terminate the stipend, and will notify the employee of the event.

POLICY NUMBER 3080: DIGITAL IMAGING SYSTEMS

PURPOSE: To describe IT Office and employee procedures and responsibilities for the use and support of Agency digital imaging systems (copiers).

POLICY: The Agency encourages the use of current digital imaging systems to maximize photocopying efficiency, and electronic document printing, production and storage. The IT Office is responsible for the purchase, installation, and configuration of digital imaging systems. Employees have certain responsibilities and are expected to follow certain guidelines in the use and maintenance of these resources.

PROCEDURES:

I. PURCHASE AND USAGE:

The Agency selects a digital imaging system vendor through a formal bid process. All new systems are obtained from the selected vendor, either through lease or purchase, and are covered by a 5-year maintenance agreement. Under these maintenance agreements, the Agency pays a cost-per-copy charge to the vendor, which provides all the necessary service, repair, and parts for the systems, including toner, but excluding copy paper.

Older Agency-owned systems are also covered by similar maintenance agreements. These systems will continue to be used until they are no longer capable of meeting employee needs.

Current digital imaging systems not only make standard photocopies, but may also contain network printing, scan-to-file, scan-to-email, and fax capabilities.

II. RESPONSIBILITY:

A. IT Office: The IT Office is responsible for working with programs to assess their digital imaging system needs, and for procuring the systems through the current vendor. In addition, the IT Office will coordinate the delivery and installation of the systems, and the training for applicable employees. The IT Office will configure the system to enable network scanning and printing functionalities, if applicable, and install the printer drivers on appropriate computers.

The vendor provides training for Agency employees free of charge. So that the IT Office is aware of employee needs and how the systems are being utilized, training requests should go through the IT Office, which will contact the vendor and coordinate training.

B. Employees: Employees are responsible for calling the maintenance provider for service and support, including toner supplies. Should a system break down or otherwise not properly function, employees are to call the appropriate maintenance provider, not the IT Office, except for problems with system network or fax functionality. The phone numbers to call for service and toner supplies are listed on a sticker on the front of each system.

For scanning, printing, or faxing problems, employees are to call the IT Office at 263-1300, which will assess the problem and either fix it or refer it to the maintenance provider.

Employees should inform the IT Office of any unresolved service and support issues, ongoing or chronic system problems, and any training needs.

POLICY NUMBER 3090: POSTAGE MACHINES

PURPOSE: To describe IT Office and employee procedures and responsibilities for the purchase, use and support of Agency postage machines.

POLICY: The Agency utilizes postage machines at selected locations to bring efficiencies and lowered costs to Agency mailing processes. The IT Office is responsible for the purchase, installation, and configuration of Agency postage machines. Employees have certain responsibilities and are expected to follow certain guidelines in the use and maintenance of these resources.

PROCEDURES: There are currently seven postage machines at various Agency locations. The current postage machines are located in Executive Office, Finance, Employment and Training, Head Start, Sanctuary, LCC, and Food Services. Program employees operate these machines as part of their mailing processes.

The Agency owns the postage machines, but rents the accompanying postage meters from third-party vendors (it is unlawful for a company to own its postage meter).

I. RESPONSIBILITY:

A. IT Office: The IT Office is responsible for replacing or adding new postage machines as needed. The IT Office is also responsible for providing the connectivity required for downloading postage into the machines (currently, via phone line).

B. Employees: Program employees are responsible for the operation of the machines, and the determination and performance of all mailing processes and procedures. Employees are responsible for ordering all supplies, including downloading of postage. Authorized employees are to call the appropriate maintenance provider for service and supplies.

POLICY NUMBER 4010: INFORMATION SECURITY

PURPOSE: To establish a policy for securing the Agency's information technology resources.

POLICY: The Agency has the right and obligation to manage, secure and control access to its information technology resources, including electronic files and data. Employees are expected to use these resources while protecting the resource's security and appropriate level of access.

REFERENCE: Health Insurance Portability and Accountability Act of 1996

PROCEDURES:

I. PROPERTY RIGHTS:

The Agency has the right to protect all information, computer and network equipment. The Agency considers as property all records, software and hardware that are part of a program's information system. As Agency property it is to be used for business purposes only. A "record" includes any information kept, held, filed, produced and reproduced by, with or for a program in any form or media including, but not limited to, reports, statements, memoranda, folders, files, books, manuals, forms, papers, maps, images, letters, photos, computer tapes and disc.

II. DISCLOSURE OF INFORMATION:

Employees are to access and use Agency information technology resources for business purposes only. Disclosure of Agency information or data to individuals or entities (whether employees or not) without a business need to have/know such information is prohibited. Agency information or electronic data may not be transmitted over the Internet or via email except for business purposes to authorized recipients. Confidential client or employee information may not be transmitted to persons or entities that are not authorized to receive such confidential information.

III. REPORTING SUSPICIOUS EVENTS:

Any observations of suspicious activity must be reported to the program's manager. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on network servers and abnormal activity recorded in log files.

IV. SECURITY TRAINING:

Agency programs are required to develop security awareness among all staff members, which includes descriptions of security breaches intended to circumvent program security management. Individual programs are responsible for the security of all Agency information resources they access. Program-specific procedures developed to conform to these policies must be reviewed frequently to reflect changes in staff and technology.

V. INFORMATION CLASSIFICATION:

Information classification provides a means for separating information into categories with different protective requirements. All programs determine the extent to which information is disclosed to specific users. The nature of the information and the duties of Agency employees determine the information classification assigned to an employee. The following categories of information serve to provide guidance in identifying appropriate users or recipients. **Public Information** is available to any person. **Restricted Information** is not public information, but can be disclosed to or used by program representatives to carry out their duties, so long as there is no legal bar to disclosure. **Confidential Information** may not be disclosed unless permitted by an Assistant Executive Director.

VI. ACCESS SECURITY:

Appropriate safeguards must be in place to limit physical access as appropriate to network, computer or computer-related devices. The IT Office is responsible for locating servers, networking equipment and other essential computer devices in an environment that protects them from unauthorized physical access.

Employees must protect their computers by logging off when unattended or by placing the computer in "lock" mode by pressing Ctrl-Alt-Del then choosing "Lock Workstation." Computer hard drives must not be shared with any other computer or person unless authorized by an Assistant Executive Director. Employees must also not leave unattended portable computing devices such as notebooks, laptops, cell phones, and PDA's, unless the device has been physically secured. When traveling, these devices should remain with the employee's carry-on luggage.

VII. REMOTE EXTERNAL ACCESS:

Remote external access to the Agency's network requires approval from an Assistant Executive Director. Usually, such access is provided to external support personnel for Agency network applications. The IT Office will provide such access and authentication methods, and log all access occurrences.

VIII. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA):

The Agency is committed to compliance with HIPAA, which provides national standards to protect the privacy of personal health information and for electronic data transmission. Any Agency program with confidential information must comply with HIPAA.

POLICY NUMBER 4020: PASSWORD PROTECTION

PURPOSE: To establish a policy concerning the use of passwords for access to the Agency's information technology resources.

POLICY: Password protection is used to provide security for Agency information technology resources and to manage access control. Password protection capability is not intended to be used by employees to protect the privacy of personal messages and files.

PROCEDURES: Passwords are required for access to numerous computer, network, and telecommunications resources, including network login accounts, GroupWise email, Finance, Human Resources, Student Information, Medical Management systems, and voicemail.

The IT Office provides employees with a login ID or username and default password to access the designated resource. Employees are then responsible to change the default password. Employees must develop a secure password not likely to be guessed. Passwords should be 6 characters or more. A combination of numbers and letters is desirable. Symbols and dashes are not accepted. The IT Office advises all employees to change passwords every 90 days or at any time they feel a password has been compromised. Employees may be required to change their Novell network login password every 90 days, when prompted.

Employees must protect the confidentiality of their passwords. Employees must not share their passwords with other persons, including other employees, or post their passwords, such as on their desks or monitors. Employees may not password protect individual files, such as Microsoft Office documents, without program manager approval, and without providing the password to the program manager. Forgotten passwords on Microsoft Office documents cannot be recovered, and the files will not be accessible. The IT Office is not responsible for issues associated with the password protection of individual employee files.

Computer boot-up passwords (BIOS passwords) are not permitted without justification and program manager approval. The IT Office will implement the boot-up password process and keep a record of the password.

Passwords do not imply that the resources they protect are private. Agency management may at any time ask for employee passwords, or direct the IT Office to change or clear employee passwords, in order to access or protect Agency information technology resources.

POLICY NUMBER 4030: VIRUS PROTECTION

PURPOSE: To establish a policy concerning the use of virus protection on Agency information technology resources.

POLICY: It is the policy of the Agency to utilize a combination of technological measures plus employee awareness and action to help protect networks, computers, and data from virus attacks and contamination.

PROCEDURES: The IT Office installs or implements virus protection measures on all Agency servers, computers, and selected network hardware. Employees also need to be aware of the dangers of viruses, and how they can help prevent virus incidents.

I. RESPONSIBILITY:

A. IT Office: The IT Office is responsible for installing or implementing virus protection software on all Agency servers and computers. The virus protection software must automatically update on a daily basis to protect against the most current viruses, and be configured for real-time protection and to “clean and notify” if it detects a virus.

Virus protection measures are also installed on the main Agency firewall and on the GroupWise email gateway, where all incoming email is scanned for viruses. These are added measures to catch viruses before they enter the network or email system.

In addition, the IT Office applies security patches and updates to servers and computers as necessary to prevent security holes and possible virus intrusions.

B. Employees: Employees can help prevent virus incidents by adopting the following procedures:

- Delete emails you do not recognize.
- Do not open any attachments you do not recognize or are not expecting, or appear to be non-work related, even if you recognize the sender’s email address. Often, malicious emails appear to come from known senders, but really do not.
- Do not attempt to alter virus protection software settings.
- Do not attempt to download or install software from the Internet or email.
- Monitor the behavior of your computer, and notify the IT Office of suspicious emails, or if your computer is sluggish, reboots on its own, or otherwise behaves abnormally.

POLICY NUMBER 4040: EMAIL AND INTERNET SECURITY

PURPOSE: To promote the safe and effective use of Agency email and Internet resources.

POLICY: The Agency will provide measures to promote the safe and effective use of email and the Internet, and expects employees to share the responsibility by following certain guidelines while utilizing these resources.

PROCEDURES: The IT Office implements various measures to combat spam, phishing, spyware, and adware, all of which disrupt the effective use of email and the Internet, and can damage email and computer systems. Employees are expected to follow certain guidelines that will help prevent and combat these intrusions.

I. SPAM:

“Spam” is electronic junk mail, or email advertising. This unwanted email wastes employee time, lessens productivity, and consumes network bandwidth. The IT Office deploys anti-spam services on the Agency’s main firewall and on the GroupWise email gateway. All traffic coming into the main Agency network is scanned for spam, as are all incoming email messages. Not all spam will be detected; “spammers” are constantly devising new ways to send their unwanted messages without detection by anti-spam devices. Employees also have the responsibility to help prevent spam and to manage any spam that reaches their GroupWise mailbox. Employees must:

- Never disclose their Agency email address to unknown parties for non-business purposes, in response to solicitations, or for other commercial purposes.
- Never input their Agency email address into any public web page, including online shopping or electronic greeting cards.
- Never respond to any spam messages received. Never click on any links within a spam message, including links with statements similar to “Click here to unsubscribe.”
- Utilize the Junk Mail Handling feature in their GroupWise account.

II. PHISHING:

“Phishing” is fraudulent email that appears to be from a legitimate Internet address, often a financial institution, usually with a request to verify the recipient’s personal information or bank account details. Agency anti-spam measures are deployed to combat phishing. Employees should simply delete these emails if received, and empty the Trash folder. Never click on the links within one of these fraudulent emails.

III. SPYWARE AND ADWARE:

“Spyware” is a general term for software that is installed on your computer, generally without your knowledge or consent, which may push out advertising, track your online behavior, or modify your computer’s settings. Spyware is a major cause of computer problems, generating unnecessary troubleshooting calls. Spyware can also gather information about email addresses and even passwords and credit card numbers. “Adware” is a form of spyware that collects information about the user’s browsing patterns in order to display advertisements in the web browser. Symptoms of spyware infection include:

- Changes to your web browser, such as extra toolbars or a different home page setting
- Changes to your browser’s security settings and favorites list
- Pop-up ads that are not related to the web site you are viewing, quite often adult content in nature
- You see advertisements when you are not browsing the Web
- Hyperlinks that do not work, or take you somewhere you did not expect)

- A sluggish system, or your system taking longer to load the Windows desktop

Spyware is downloaded from the Internet onto the computer. It is often attached to other files that you have chosen to download, or it can be downloaded when you click on banner ads on web sites.

Types of downloads from the Internet that may contain spyware include:

- Games
- Music, movies, or other file-sharing programs
- Themes and characters for your desktop
- Screen savers
- Toolbars for Internet Explorer web browser
- Free pop-up blockers that appear while you are online

Employees can prevent spyware by simply not downloading software from the Internet. It is against Agency policy to download non-business related material from the Internet. In addition, employees should surf the web safely by never clicking on any links that say "I agree" or in response to any pop-up ads or messages.

The IT Office combats spyware through the use of anti-spyware and intrusion detection software on the main Agency firewall. In addition, workstation virus protection software also scans for spyware and adware. When necessary, the IT Office will install workstation anti-spyware software to clean up and/or prevent individual computer spyware infections.

POLICY NUMBER 4050: SYSTEM ACCESS

PURPOSE: To establish security controls for granting employees access to the Agency network, system applications, and phone and voicemail.

POLICY: Agency program management is responsible for determining the access requirements of its employees, and communicating these requirements to the IT Office. The IT Office will work with the programs to implement the security access required, according to proper procedures.

PROCEDURES:

I. NEW EMPLOYEES:

To add a new employee to the Agency network, an Assistant Executive Director or designee must inform the IT Office in writing, providing the employee's full name, job title, program, location, telephone number, fax number, and start date, and whether the new employee should have a GroupWise email account. The IT Office will create a network account and GroupWise account, if applicable, for the new employee, using the naming convention of first name initial and full last name (up to 8 total characters), i.e. "jsmith" for John Smith.

In addition, the IT Office must be notified in writing of any other access requirements the employee may need, such as to "group" folders on the network, specific network printers, or to specific program's network systems, such as Finance, Human Resources, Student Information System, Medical Management System, etc. The IT Office will ensure that the proper software is installed on the employee's computer, establish the proper network access rights, and will work with the programs as applicable to create separate usernames and passwords for these systems.

The IT Office will also assign a phone number and create a voicemail account, if applicable, for the new employee.

II. STATUS CHANGES:

So that appropriate security changes can be made, an Assistant Executive Director or designee is responsible for reporting in writing to the IT Office changes in employment status or job duties of their employees. Employees in new positions or with new duties may not need the same access as they had before, and they should only have access to those resources for which they have a legitimate business need.

III. DELETIONS:

An Assistant Executive Director or designee is responsible for notifying the IT Office in writing of employee network and GroupWise accounts that need to be deleted, whether for termination or other cause. The IT Office will delete employee network and GroupWise accounts immediately upon notification after an employee's termination, except as directed by an Assistant Executive Director. An Assistant Executive Director must approve keeping the accounts open. However, the IT Office will immediately upon notification change the passwords of terminated employees in order to protect the security of the network and email system.

The IT Office will work with appropriate program staff to delete terminated employee's login accounts on individual network applications.

POLICY NUMBER 4060: DATA BACKUP AND RECOVERY

PURPOSE: To ensure data stored on Agency file servers is backed up on a daily basis and to be able to recover the data in case of a disaster or other event causing data loss.

POLICY: It is the policy of the Agency to perform a backup of each server after the close of business, each night Monday through Friday, and to perform a test restore for each server at least quarterly to ensure the recoverability of the data on the backup tapes. The IT Office is not responsible for the backup of files located on employee computer hard drives.

PROCEDURES: Designated IT Office staff is responsible for performing daily backups of the servers located at 1920 Mariposa Mall. Backups of "off-site" servers located at program sites are the responsibility of designated program staff. Data is backed up onto tape media (cartridges) loaded into tape drive devices attached to the servers.

For each tape drive device there are 15 individual tape cartridges to be used in a 15-day (3 week) rotation. Each tape is numbered 1-15 with the day of the week, i.e. #1 Monday, #2 Tuesday...#6 Monday, etc. After tape #15 Friday is used, the rotation begins again from tape #1 Monday, overwriting the data previously backed up onto tape #1 Monday. All tape cartridges are thus overwritten every 15 days. The tape cartridges are stored next to the tape drives in a secure area.

Through the configuration of the backup software application, backups are scheduled to run each night after the close of business, and are completed by the beginning of the next business day.

1. For each tape drive device, responsible staff will, no later than the close of the business day, remove the backup tape cartridge representing the previous business day's backup from the tape drive and insert the tape cartridge to be used for the next backup process. For example, on Monday, staff will remove the tape used for Friday night's backup (i.e. #5 Friday), and insert Monday's tape (#6 Monday).
2. Responsible staff will take the removed tape cartridge offsite. Staff will return the tape cartridge on the third business day following the date of backup. For example, a tape containing Monday night's backup will be taken offsite by the end of the day on Tuesday, and returned on Thursday. The returned cartridge will then be ready for its next turn in the rotation. This will ensure that there will always be at least one tape backup cartridge offsite at all times.

For the tape drives located at 1920 Mariposa Mall, responsible IT staff will place the removed tape cartridges in a locked, fireproof cabinet located at 1900 Mariposa Mall, Suite 121. The tape cartridges will be then be retrieved from the cabinet and returned on the third business day following the date of backup.

3. Responsible staff will complete the Backup Tape Log on a daily basis, recording backup dates and initialing the removal and returning of the tape cartridges.
4. Responsible IT staff will use the backup software's reporting utilities at the start of each business day to validate the accuracy, completeness, and integrity of the backup performed the previous night.
5. Any errors will be acted upon in a manner commensurate with the type of error. Responsible IT staff will use contract technical support as needed to resolve problems and ensure the validity of backup data.

6. Responsible staff will clean the tape drive device at least twice a month, using appropriate tape cleaning cartridges.
7. Responsible IT and/or program staff will ensure replacement of backup tape cartridges as needed.
8. The IT Office will perform file/data restores from the tape cartridges as requested by staff, and log successful restore functions. Any problems identified during the restore function must be acted on in a timely fashion. Responsible staff will use contract technical support as needed to resolve problems and ensure the validity of backup data.
9. The IT Office will ensure that restores, whether test or for actual data loss, are performed for each server at least quarterly.

POLICY NUMBER 5010: COMPUTER HARDWARE STANDARDS

PURPOSE: To promote high levels of technological compatibility, performance and efficiency and to ensure that the Agency stays current with industry standard technology.

POLICY: The IT Office selects specific computer hardware standards for business need, stability, proven effectiveness in the workplace, cost-effectiveness, ease of use and ease of support.

PROCEDURES:

I. DESKTOP COMPUTER HARDWARE:

Minimum Standards for New Purchases

HP Compaq Pentium 4, 2.8Ghz
Mini or mid-tower case
40GB hard drive
512MB RAM
17" LCD multimedia monitor
10/100 NIC
CD-ROM, keyboard, mouse
No floppy drive, DVD drive, or CD-burner

II. LAPTOP/NOTEBOOK HARDWARE:

Minimum Standards for New Purchases

The Agency purchases Toshiba laptops and notebooks. The exact features and configuration, especially screen size, in large part depend upon the intended use of the laptop or notebook, and on the preference of the employee. The IT Office will work with the employees to select the appropriate model and configuration of each. In general, most laptops and notebooks purchased will have the following minimum standards:

Toshiba Satellite or other model
Intel Centrino Mobile Technology
Intel Core Solo Processor
512 MB RAM
14.1" diagonal XGA display
80GB hard drive
DVD/CD-burner
10/100 NIC
802.11a/b/g wireless

The appropriate program authority and the IT Office must approve any exceptions to the published standards. In addition, programs are not to accept donations of computer equipment from outside entities. The IT Office must first be notified of the availability of such donations. The IT Office will then ascertain the specifications of the equipment to determine compatibility with Agency standards and useability, and will make a determination to accept or reject the donation.

To stay current with industry developments, Agency computer hardware standards may change.

POLICY NUMBER 5020: COMPUTER HARDWARE INSTALLATION AND MAINTENANCE

PURPOSE: To promote efficient and expeditious computer hardware installation, and to promote computer hardware stability and longevity.

POLICY: The IT Office is responsible for all computer hardware installations, and will install and maintain the equipment in the most efficient and cost-effective manner feasible. Employees are also expected to protect and help keep the hardware safe and clean.

PROCEDURES:

I. INSTALLATION:

The IT Office sets up and installs all computer hardware, and will work with authorized program staff to determine the best location. The IT Office is not responsible for obtaining or setting up computer desks or other furniture. Locations must be prepped and ready, including electrical, before the IT Office can set up the hardware.

So that the Agency may keep track of its computer resources, the IT Office assigns a computer name for all employee desktop computers, affixes a label with the computer name onto the computer case, and inventories the hardware (and software installed), including the name of the employee assigned to the computer. Employees may not move the computers to other locations or change the employee assigned without IT notification, participation, and proper program approval.

II. MAINTENANCE:

Employees may request technical support for hardware issues by contacting the IT Office as described in procedure 7010, "Service Requests." The standard warranty for Agency computer hardware is 1-year parts and labor, on-site limited warranty. The programs are responsible for paying for repairs that are needed outside of the warranty period. Often, this only applies to the purchase of the parts needed, as the IT Office can perform the needed repairs. The IT Office *may* be able to provide spare parts in cases of emergency, but there is no guarantee. Programs are responsible for the purchase of all repair parts and any needed accessories, including keyboards, mice, USB cables, surge protectors, power strips, etc.

Computer upgrades beyond the addition of additional memory are generally not cost effective, or technically possible or advisable. The IT Office generally recommends replacing older, under-performing computers with new ones rather than attempting to upgrade.

Employees are responsible for protecting the computer equipment they are utilizing, and to keep the equipment clean. Special care should be taken with food and drink. Computer equipment that is in an unsafe location should be brought to the attention of program management and the IT Office. With proper care, Agency computer equipment can serve the needs of employees for at least three years. At the time the equipment is considered obsolete, the IT Office will recommend replacement, but individual programs must budget and pay for any new equipment.

POLICY NUMBER 5030: COMPUTER HARDWARE DISPOSAL

PURPOSE: To set a policy for the proper and lawful disposition of obsolete computer equipment.

POLICY: It is the policy of the Agency not to keep computer equipment longer than its useful life, and to dispose of it properly through donation or proper and lawful recycling procedures.

REFERENCE: California e-Waste Collection and Recycling Act, Senate Bill 20

PROCEDURES: Neither the IT Office nor programs will keep or store for an extended period of time computer equipment that has been replaced or is obsolete. The IT Office will not use equipment considered obsolete elsewhere in the Agency. Computer or other electronic equipment must not be thrown in the trash or dumpster, except for mice and keyboards. When computer equipment is identified as obsolete, the following procedures are to be followed:

1. An Assistant Executive Director or designee will contact the funding source to determine if there are any disposal restrictions. If there are no restrictions, then the AED or designee will inform the IT Office in writing of approval to dispose of the equipment.
2. The IT Office will note the description, model, serial number, and Agency property tag number (and remove the tag), if applicable, of each piece of equipment.
3. The IT Office will assist the employee with saving any files needed on hard drives, then sanitize the hard drives using industry standard software.
4. The IT Office will move the obsolete equipment to an appropriate location for temporary storage.
5. If the equipment can be donated to outside organizations or individuals, and such recipients are readily available, then the IT Office will facilitate the scheduling of the donation.
6. If the equipment cannot be donated, then the IT Office will contact the FCEOC Local Conservation Corps Recycling Manager. LCC is a certified, designated e-waste collector. LCC will pick up on a scheduled date and time all the equipment ready to be recycled. Such equipment can include: CRT and LCD monitors, computer systems, printers, scanners, keyboards, mice, fax machines, hard drives, Uninterruptible Power Supplies, and most other kinds of electronic equipment, including cell phones.
7. LCC will pick up the equipment and recycle according to its policies and procedures.
8. The IT Office will provide the Assistant Finance Director/Programs and Audit with the list of equipment from #2 above.

POLICY NUMBER 5040: NON-AGENCY COMPUTER HARDWARE

PURPOSE: To protect the Agency's network systems from viruses and other security breaches, and to ensure only Agency resources are used for Agency business activities.

POLICY: It is the policy of the Agency that non-Agency computer hardware, including employees' personal computer equipment, may not be installed in or used on Agency computer or network systems.

PROCEDURES: To ensure compliance with this policy, all computer hardware and equipment installed in or used on Agency computer and network systems must be Agency-owned. This includes, but is not limited to, personal computers, laptops, notebooks, flash drives, external hard drives or CD-burners, network hubs or switches, wireless routers or access points, printers, monitors, scanners, keyboards, and mice. Employees may not bring in any such equipment from home for utilization at the Agency.

Exceptions to this policy are reserved for outside auditors and monitors representing funding sources, or for meeting presenters from outside agencies. However, the IT Office must be notified of these exceptions, and before such outside equipment can be used at the Agency, the IT Office must certify with the outside persons that their equipment does not represent a threat to Agency network systems, and that their computers have the appropriate Windows security patches and updated virus protection software.

POLICY NUMBER 6010: COMPUTER SOFTWARE STANDARDS

PURPOSE: To promote high levels of software compatibility, performance and efficiency and to ensure that the Agency stays current with industry standard software.

POLICY: The IT Office selects specific computer software standards for business need, stability, proven effectiveness in the workplace, cost-effectiveness, ease of use and ease of support.

PROCEDURES:

Standard Desktop Software Configuration:

- Windows XP SP2 (new) or Windows 2000 Professional (legacy) operating system
- Microsoft Office Professional:
 - Word (word processing)
 - Excel (spreadsheet)
 - PowerPoint (presentations)
 - Access (database)
 - Publisher (graphics, flyers, brochures, etc.)
- McAfee VirusScan Enterprise (virus protection)
- Novell GroupWise (E-mail, collaboration and calendaring)
- Novell GroupWise Messenger (instant messaging)
- Microsoft Internet Explorer 6.0 or above (web browser)
- TightVNC (remote desktop support)
- Adobe Acrobat Reader (.pdf document reader)
- Windows Media Player (multimedia)
- Novell Client for Windows (network connectivity)

An Assistant Executive Director and the IT Office must approve any exceptions to the published standards. To stay current with industry developments, Agency computer software standards may change.

POLICY NUMBER 6020: COMPUTER SOFTWARE INSTALLATION AND MAINTENANCE

PURPOSE: To promote optimal computer configuration and operation, and to prevent unauthorized software from being installed on Agency computers.

POLICY: Only IT Office staff may install software on Agency computers. All such software must be properly licensed.

PROCEDURES:

I. INSTALLATION:

The IT Office is responsible for configuring Agency computers with standard software applications and any additional program-specific software. Employees may not install or delete software without IT Office approval or assistance. The IT Office reserves the right to place controls on Agency computers to restrict or prevent unauthorized software installations, or modifications to the Windows operating system or to other installed software. Such controls may include:

- Windows workstation profile restrictions
- Windows Microsoft Management Console configuration
- Security software, such as Deep Freeze or other software to prevent the installation or modification of Windows operating system or other computer software.

II. MAINTENANCE:

A. Technical Support: Employees may request technical support for software issues by contacting the IT Office as described in procedure 7010, "Service Requests." In the course of addressing any software issue, the IT Office may decide the best solution is to "re-image" the computer (to take the computer back to a clean, "default" software configuration), which will delete all files on the hard drive. The IT Office will make its best effort to save employee files on hard disks before re-imaging the computer. The IT Office will not re-install any personal or unapproved non-standard software that may have been on the computer.

B. Maintenance Agreements: The Agency enters into software maintenance agreements as needed to ensure continued technical support for a critical software product, and to be entitled to the latest versions of the software. The Agency has software maintenance contracts for Novell NetWare/Open Enterprise Server, Novell GroupWise, McAfee VirusScan, Financial Edge Accounting for Non-Profits, GE Centricity Practice Management System, PowerSchool Student Information System, ChildPlus, iVantage Human Resources Information System, and other critical program-specific software applications.

C. Licensing: Regardless of any software maintenance agreements, all Agency programs and employees must adhere to all licensing agreements and software copyright laws. The IT Office has the right and obligation to conduct a software inventory of all Agency computers at regular intervals and as-needed to ensure compliance. Unauthorized software will be removed.

POLICY NUMBER 6030: NON-AGENCY COMPUTER SOFTWARE

PURPOSE: To protect the Agency's network and computer systems from the unknown effects of non-Agency software, and to comply with software licensing agreements and copyright laws.

POLICY: It is the policy of the Agency that non-Agency software, including employees' personal software, may not be installed in or used on Agency computer or network systems.

PROCEDURES: To ensure compliance with this policy, all computer software installed in or used on Agency computer and network systems must be Agency-owned. Employees may not install personal software on Agency network or computer systems, and may not download and install software from the Internet, even if it is "freeware," (software available for free), or "shareware," (software available for free, but a small fee is requested by the author if used regularly). Both freeware and shareware are copyrighted by the author.

Any exceptions to this policy require Assistant Executive Director and IT Office approval.

POLICY NUMBER 7010: SERVICE AND SUPPORT REQUESTS

PURPOSE: To define policies and procedures for employee service and support requests and IT Office response.

POLICY: It is the policy of the Agency that employee requests for service and support are streamlined and addressed in a timely manner, based on priority and available resources.

PROCEDURES:

I. PLACING SERVICE AND SUPPORT REQUESTS:

Employees are encouraged to contact the IT Office to request service and support for computer or network issues. All Agency employees can request service and support for the following:

- Assistance with computer applications
- Network or email login problems
- Printing/printer problems
- Hardware troubleshooting

Certain requests for IT Office support must come from a Program Director or above. Examples include the following:

- Any requests relating to file access permissions
- Replacing or moving equipment, office reconfigurations
- Creation of new accounts
- Installation of new software

In addition, individual programs may have their own guidelines for requesting IT Office support, which employees are required to follow.

Employees may open a service and support request by contacting the IT Office as follows:

- Phone: 263-1300
- Email: itoffice@fresnoeoc.org

II. MANAGING SERVICE AND SUPPORT REQUESTS:

The IT Office utilizes TrackIT! help desk management software to generate work orders and track all requests, large or small, for IT support. The following procedures are followed when processing a service and support request:

1. The request is input into TrackIT! as a new work order, prioritized, and assigned to the appropriate IT Office staff. The IT Office may not be able to respond to the request immediately, depending upon the priority of the issue or the number of existing open requests that are pending.
2. The IT Office will troubleshoot the issue with the employee. Troubleshooting steps may include working with the employee over the phone, and requesting the employee to perform certain troubleshooting steps under the IT Office's instructions. The issue may require an on-site support visit by the IT Office. Programs and employees should make their computers available to the IT Office whenever necessary.
3. The IT Office will utilize remote desktop support whenever possible to troubleshoot the issue, in order to save time and expense. The IT Office can remotely access and take control of an employee's computer using TightVNC remote access software. As a courtesy, the IT Office will notify the employee when remote access will be used. If the

employee is not available, the IT Office will attempt to notify the employee's supervisor or other program supervisor.

4. All troubleshooting steps and results are logged into the work order. When the issue is resolved, the completion date and time is noted in the work order.
5. The IT Office makes every effort to resolve all issues in a timely manner; however, due to such variables as equipment, licensing, and budget constraints, for example, some requests cannot be immediately granted or solved. For example, hardware and software problems with older computers may not be able to be fixed until newer hardware is purchased. In addition, the complexity of the issue may require technical support from outside service providers.

POLICY NUMBER 7020: SERVICE PROVIDERS

PURPOSE: To communicate the situations and procedures in which outside service providers are enlisted to provide service and support to the Agency.

POLICY: It is the policy of the Agency to utilize the services of outside service providers when necessary to provide maintenance, service, and support for Agency information technology systems and resources.

PROCEDURES: Outside service providers provide support services to the Agency under various conditions and situations. All outside service providers must be approved by the IT Office and/or appropriate executive management (in cases of maintenance agreements). The Agency may use the services of outside service providers under the following scenarios:

I. SERVICE/MAINTENANCE AGREEMENTS:

The Agency has entered into service or maintenance agreements with a number of outside service providers, usually with software vendors to ensure continued technical support for their software products, and to be entitled to the latest versions of the software. Such agreements exist for the following systems: Novell NetWare/Open Enterprise Server, Novell GroupWise, McAfee VirusScan, Financial Edge Accounting for Non-Profits, GE Centricity Practice Management System, PowerSchool Student Information System, ChildPlus, iVantage Human Resources Information System, and other critical program-specific software applications. In addition, the Agency's main access to the Internet is through McMillan Consulting, an outside Internet Service Provider (ISP).

The IT Office will contact the contracted service provider when necessary to address and fix problems, apply updates, or otherwise to provide assistance. Depending upon the individual system affected, authorized program employees may directly contact the service provider with technical support questions. However, employees must keep the IT Office informed of such requests and their progress, and employees may not make any changes to the network or system while troubleshooting. Any required modifications to the network or to the system need to be performed either by the service provider with the knowledge of the IT Office, or by the IT Office.

II. WARRANTIES:

The IT Office will utilize the manufacturer's warranty when active to fix or repair hardware problems. This may entail on-site support from technicians representing the manufacturer. In most cases at the Agency, they will be representing Hewlett-Packard or DELL. The standard warranty for Agency computer and network hardware is 1-year parts and labor, on-site limited warranty. Server hardware carries a 3-year on-site warranty.

III. AS NEEDED:

The IT Office will also enlist the services of outside service providers on a chargeable, case-by-case basis, when the complexity of the problem exceeds IT Office resources. These situations occur infrequently, and are usually related to Agency network and server system problems.

POLICY NUMBER 7030: IT TRAINING

PURPOSE: To enhance employee expertise in Agency-standard software applications.

POLICY: The Agency provides in-house IT training classes for employees to assist them in acquiring the appropriate level of software application knowledge to perform their duties in an effective and efficient manner.

PROCEDURES: The IT Office provides IT training classes in the IT Training Room, located at 1920 Mariposa Mall, Suite 350. The classes begin at 8:45 a.m. and end at 12:15 p.m. Notebook computers are provided so each employee will have hands-on training. Employees interested in the IT Office's in-house training classes may check the classes and schedule available by checking the Agency's Intranet site, checking the "IT Training Room" calendar in GroupWise, or by calling the IT Office at 263-1300. Employees may sign up by calling the IT Office at 263-1300 or by emailing the "IT Training Room." The classes offered are:

- GroupWise 6.5 (full)
- What's New in GroupWise 6.5?
- Introduction to Computers
- Mail Merge/Tables
- MS Access 2000 (Beginning, Intermediate)
- MS Excel 2000 (Beginning, Intermediate)
- MS PowerPoint 2000 (Beginning, Intermediate)
- MS Word 2000 (Beginning, Intermediate)

The IT Office will also work with programs to offer customized training classes to fulfill specific needs.

I. REQUESTING TRAINING CLASSES:

A. Intranet Site: To find training information on the Intranet site:

1. Go to www2.fresnoeoc.org
2. Click on the "Information Technology" menu section at the top of the screen.
3. Click on the "Training and Support" menu option to the left of the screen.
4. Under the sub-heading "Training," click on the "IT Training Schedule" link.
5. A list of training classes with a tentative date should be displayed. Employees should review the list and choose the classes they wish to take.
6. Call the IT Office at 263-1300 to schedule the training, or email your request to the "IT Training Room."

B. IT Training Room Calendar: To find training information within GroupWise,

1. Open your GroupWise account
2. Click on the "Online" button above your mailbox name.
3. Choose "Proxy."
4. Select the "Address Book" icon to the right of the name box.
5. In the "Look for" box, type "IT"
6. A list of names beginning with "IT" should appear. Find and select "IT Training Room."
7. Press "OK."
8. Your mailbox should change to "IT Training Room."
9. Click on Calendar. Potential training classes are scheduled on Tuesdays, Wednesdays, and Thursdays.

10. Find the class you wish to take, and call the IT Office at 263-1300 to schedule the training, or email your request to the "IT Training Room."

C. Calling the IT Office: To find training information via phone, call 263-1300 and inform the receptionist that you are interested in taking computer training classes. Make sure you know which class(es) you would like to take.

II. SCHEDULING TRAINING CLASSES:

Once the IT Office is informed of the request for training, the IT Office will schedule the employee(s). Once the class and date is confirmed, a GroupWise appointment will be emailed directly to the employee(s) to schedule the requested training class, and their supervisor will be copied. Upon receiving the appointment email, employee(s) should "accept" the appointment. By accepting the appointment, the appointment will be placed within the employee's calendar in their GroupWise account. A reminder email will also be sent to the employee(s) and supervisor one day before the scheduled class.

III. PREREQUISITES:

Employees must receive permission from their supervisor to take IT training classes, and it is preferable that supervisors work with the IT Office to schedule classes for their employees. The IT Office will assume that all employee requests for training received have been approved by the employee's supervisor.

Employees must have working knowledge of computers and computer applications to take the MS Office and GroupWise courses, and will need to take the classes in a logical order, i.e. Beginning MS Word before Intermediate MS Word). The IT Office reserves the right to ascertain the knowledge level of employees to ensure that they are placed in the correct class.

IV. RESTRICTIONS:

IT training classes have restrictions on class size. The minimum number of employees is four, and the maximum is six. The IT Office may, at its discretion, cancel classes with less than four employees, and re-schedule the class at a later date. Class size may exceed six at the discretion of the IT Office, but employees should expect to share a notebook computer. Employees interested in IT training classes should attempt to enlist their co-workers so that there are enough interested employees to have a class.

V. TRAINING COMPLETION:

At the end of each training class, each employee must complete an evaluation form indicating their satisfaction with training, recommendations, and if they are interested in taking future training classes. The evaluations are compiled for review, and filed away for future use.

The names of the employees and classes taken are recorded in the IT Office's TrackIt! help desk software, so a record is kept of the courses employees have successfully completed.

POLICY NUMBER 7040: IT PURCHASING

PURPOSE: To establish uniform policies and procedures in the purchasing of information technology equipment, software, and services.

POLICY: All purchases of information technology equipment, software, and services will be purchased through, or with the assistance of, the IT Office. The IT Office will adhere to Agency policies and procedures in making information technology purchases.

REFERENCE: FCEOC Accounting Policies and Procedures Manual, Purchasing

PROCEDURES:

I. DEFINITION:

Information Technology equipment, software, and services includes:

Equipment:

- Network equipment and services
- Servers
- Telephone equipment
- Video equipment
- Computers
- Printers, Scanners
- Fax machines
- Digital imaging systems (copiers)
- Cabling and phone and data circuits
- Other electronic devices

Software:

- Computer software applications
- Network software applications
- Phone and voicemail software applications

Services:

- Internet services
- Telephone services

II. PROGRAM-INITIATED PURCHASES:

Programs desiring to purchase information technology equipment, software, or services will contact the IT Office. Appropriate program and IT Office staff will review the need and request, and arrive at the recommended information technology items to purchase.

The IT Office will obtain price quotes for the desired items per Agency purchasing procedures. Once obtained, the IT Office will document the price quotes, recommend a vendor, complete a purchase order and present the documentation and purchase order to the appropriate program authority for review and approval. The program will return the signed purchase order to the IT Office, which will submit the purchase order to the selected vendor.

After all of the items have been delivered and the invoice received, the IT Office will sign the invoice confirming receipt of the items, and forward the invoice to the appropriate program staff for signature. The programs are responsible for forwarding the signed invoice, purchase order, and supporting documentation to Accounts Payable for payment to the vendor.

III. IT OFFICE-INITIATED PURCHASES:

IT Office-initiated purchases also must follow Agency purchasing procedures. These types of purchases are for equipment, software, and services that benefit programs Agency-wide. The IT Office researches the need, reviews options, and recommends the desired equipment, software and other related items needed by the Agency for its normal course of operations. The IT Office must acquire at least three bids when procuring new equipment or services. Once obtained, the IT Office will document the price quotes, recommend a vendor, complete a purchase order and present the documentation and purchase order to the appropriate Assistant Executive Director or authorized designee for approval. Once approved, the IT Office will contact the vendor and place the order.

After all items have been ordered and delivered, and the invoice received, the IT Office will sign the invoice confirming receipt of the items, and forward the invoice to the appropriate signing authority for signature. The IT Office will then forward the signed invoice, purchase order, and supporting documentation to Accounts Payable for processing.