Mono County

PC Policy and Procedures Statement

Index

Mono County PC Policy and Procedures Statement

The General Philosophy

To encourage cost-effective applications of PC technology; allow end users every opportunity to acquire hardware and software, and coordinate the recommended software and hardware with education, consulting support and sharing of experience and applications. It is also essential to establish procedures for acquiring PC's and to assign clear responsibility for audit ability, security, and where relevant, maintenance.

Computer Ethics Policy

Many users share the computer facilities at Mono County. Most people use these resources responsibly. However, a few users who misuse the computing facilities have the potential for disrupting the work of other users. You are expected to exercise responsible, ethical behavior when using the Mono County computing facilities. This includes the following:

- You must use only the computer accounts which have been authorized for your use by Mono County. The unauthorized use of another's account, as well as the providing of false or misleading information for the purpose of obtaining access to computing will be treated accordingly by Mono County.

- You may not authorize anyone to use your account(s) for any reason. You are responsible for all usage on your accounts. You must take all reasonable precautions, including required password maintenance and file protection measures, to prevent use of your accounts by unauthorized persons. The only exception to this would be IT personnel working on a problem for you.

- You must use your accounts only for the purposes for which they were authorized. You must not use your accounts for unlawful purposes, such as downloading, installation, use of fraudulent or illegally obtained software.

- You must not access or copy files (including programs, members of subroutine libraries, and data) that belong to another account without prior authorization of the account holder. Files may not be taken to other computer sites without permission from the holder of the account under which the files reside.

- You must not use the system irresponsibly, or needlessly affect the work of others. This includes the transmitting or making accessible offensive, annoying or harassing material; intentionally damaging the system, or information not belonging to you;

intentionally misusing system resources such as personal facebook, twitter, hotmail web access, etc., or allowing misuse of system resources by others.
Note: The use of facebook, twitter, etc. can be used for business purposes such as promoting the County or County programs. The internet access is a very powerful tool, a privilege, and is available for business purposes only.

- You are responsible for reporting to the Information Technology Department, any violation of these guidelines by another individual. You are also encouraged to report any information relating to a flaw in, or bypass of, computer facilities security.

Failure to comply with the above guidelines, or the unauthorized or illegitimate use of Mono County's computing facilities or resources, shall constitute a violation of County policy and will subject the violator to disciplinary or legal action by the County. In addition, the County may require restitution for any use or loss of service, which is in violation of these guidelines. Any questions about this policy or of the applicability of this policy to a particular situation should be referred to the Information Technology Department.

The "ALL" Email Account – The all email account is a restricted use account. It is for business purposes only. If you need to use this account it must be cleared by your department head and the IT Director or the CAO.

Working from Home – We have the capability to allow you to access your work computer from home. In order for IT to facilitate this privilege you must obtain written approval from the CAO and forward a signed copy to the IT email account (Support@MONO.CA.GOV). This process will initiate a workorder to set you up.

Password Policy

- Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Mono County Governments entire network. As such, ***all Mono County Government employees (including contractors and vendors with access to Mono County Government systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.***

- The purpose of this policy is to establish a **standard for creation of strong passwords, the protection of those passwords, and the frequency of change.**

- The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Mono County Government facility, has access to the Mono County Government Network, or stores any non-public Mono County Government information.

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every 30 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

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

Poor, weak passwords have the following characteristics:

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

Strong passwords have the following characteristics:

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

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

Password Protection Standards

Do not use the same password for Mono County Government accounts as for other non Mono County Government access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, **don’t use** the same password for various Mono County Government access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share Mono County Government passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Mono County Government information.

Here is a list of "don’ts":

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

- If someone demands a password, refer them to this document or refer them to the Information Technology Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).
Again, **do not** write passwords down and store them anywhere in your office. **Do not** store passwords in a file on any computer system (including Palm Pilots or similar devices) without encryption.
Change passwords every 30 days
If an account or password is suspected to have been compromised, report the incident to the Information Technology Department immediately and change all passwords.
Password cracking or guessing may be performed on a periodic or random basis by the Information Technology Department.
If a password is guessed or cracked during one of these scans, the user will be required to change it immediately.

Use of Passwords and Pass phrases for Remote Access Users

Access to the Mono County Government Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

Pass phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.
Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is somewhat more secure against "dictionary attacks."
A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"
All of the rules above that apply to passwords apply to pass phrases.

Enforcement

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

Request for Service Procedure

1. To schedule service from the IT department call (760) 932-5500 or send an email to Support@mono.ca.gov. This email should describe the problem to the best of your ability including who to contact and the contact phone number.
2. IT personnel will take the pertinent information and create a work order.
3. A response to the call will be made as soon as possible.

We understand all calls are important and you need your computer. Keep in mind we are fielding other calls and we will get to you ASAP. If you have a true emergency please let us know the circumstances. We have limited staff and cannot treat every call as an emergency.

Note: Due to the nature of the services provided by the Sheriff's Department, the IT department will give the Sheriff's Department preferential consideration to requests for computer service and support.

IT personnel will be available on an on-call basis during regular business hours, 8:00am to 5:00pm, Monday through Friday at 932-5500. The Sheriff's Office will be provided emergency support after hours. Emergencies are defined as issues of a critical nature that cannot wait until the next business day. After hours contact telephone numbers and schedule will be provided to the Sheriff's Office under separate cover.

Principles for Determining Need for Upgrades

- No existing computer, with adequate resources, is available to transfer to the employee.
- The current system is inadequate. A system is inadequate if it will not run the software required to perform the employee's job tasks. Examples would include:
  - A hard disk is full and cannot load a software upgrade or a specialized software is required that will not fit on the existing disk.
  - Inadequate memory causes extremely slow operation or memory is required for a software upgrade.
  - Inadequate processor speed to reasonably handle the work requirement.

Upgrades

- The County will purchase the most cost efficient upgrade available that is compatible with user needs. Factors that influence the type of upgrade needed include:
  - Availability of funds.
  - The age of the computer.
  - The cost of the needed upgrade (occasionally it is more cost effective to purchase a new machine instead of individual components).
  - The types of applications the operator is running now or plans to run in the future requiring additional computer resources.

    - **Note**. In order for the County to maintain technological parity, it is important to budget for replacement PC's every five years, ie: If there are 5 computers in the department, one computer per year should be budgeted with a plan to cycle out the least effective machine.

Purchase Procedure for New Computers or Upgrades

- The IT department will serve as coordinator for the purchase/acquisition of all County PC hardware and software. (see note *)

- A standard PC configuration will be ordered for each approved and budgeted request, if it is not feasible to upgrade the existing computer. The standard configuration will be determined by IT personnel. The standard will always be improving, because of technology changes. All computers will be configured for e-mail, and the internet. If you do not want a computer set up to access the internet please let us know in the approval letter for the purchase.

- Users who wish to acquire hardware and/or software must register their requests with the IT department through their department head by email with an approved account number to charge. The request should be budgeted in the user department budget. The request will be reviewed, recommendations made and the order will be submitted.

- Those who need hardware/software, above and beyond the standard, should indicate the need on their request along with the business justification.

- All PC's will be shipped to the IT Department for "setup" and software installation before delivery to the user department. (see note *)

- IT will make every effort to get the best price and equipment for the County.

- To decrease the purchase demands on the County Budget, departments should include computer hardware, software, and support requests when applying for grants.

Note* Exceptions are State and Federal Grants, Agencies or Programs that dictate hardware and software requirements. In such cases, the subject department shall handle the ordering of and delivering to that departments location. IT will provide set-up services as requested.

Backup Policy

Backup of servers located at the County IT facility and the Sheriff's IT Facility are the responsibility of the IT department. These backups will occur on a weekly or daily basis depending on the application and need. Backups will be rotated and recycled on a regular basis. If a Department requires a permanent backup, it is their responsibility to work with IT and see that the backup is completed. IT will be glad to assist with these needs. One of the weekly and one of the daily backup devices will be stored in a secure fireproof vault on site at the Sheriff's administration and in an offsite location for the County devices.

Servers **not located in the IT facility** are the responsibility of the department owning the server. Thus, each department is responsible for backing up their own server. IT will work with you to set up procedures for this process.

We do not recommend storing valuable files on a local drive on your PC. Should you do this it is **your responsibility to backup** the files on a regular basis.

The purpose of the backups is to safeguard user and system files against accidental erasures and other mishaps. **Backups are not done to provide an indefinite storage of the information existing on the computers.** These backups are rotated on a regular basis and eventually overwritten. Any information the users wish to maintain for a very long or indefinite period, should be backed up by the users themselves and stored in a safe place. IT will assist if necessary.

Responsibilities:

1. Users are responsible for obtaining approval for acquisitions from their management.

2. Further user responsibilities include the following:
   - Compliance with all legal and audit requirements.
   - Reasonable security of hardware, software, and data including site security.
   - Data integrity. No user application may update a database created or stored on a remote machine. If such a capability is justified, it must have the concurrence of IT. "Remote machine" is defined as a PC or server not belonging to the user department.
   - Report integrity. In situations where a PC report has basically the same format as an official report, the user must make sure the two cannot be confused.
   - Ethics. Piracy is a growing problem for software vendors. Users are responsible for ensuring that the spirit and letter of the laws of copyright and trademark protection are followed to protect both the individual and the County. Using, utilizing, copying or otherwise distributing County purchased applications is strictly prohibited. See Computer Ethics Policy on page 3.

3. The IT department is responsible for assisting users in the following areas of acquisition and application of PC technology:
   - Purchasing
   - All software installation
   - Maintenance
   - Troubleshooting
   - Network administration
   - Server administration
   - E-Mail administration
   - Internet access
   - Basic training for users
   - Identifying and evaluating new software and hardware and adding items to the recommended list.
   - Telephone administration

Definitions:

Standard Hardware:
Processor
Local disk/Hard drive
CD ROM/DVD
Network Card
Monitor
UPS/Surge Protector
Mouse
Keyboard

Hardware Options:
CD/DVD writer
Scanners
Printers
Docking Station (for Laptops)
Monitor (option for docking station)
External Mouse (for laptops)
Power adapters (laptops)
External keyboard (for laptops)
Extra battery (for laptop)

Standard Software:
Latest Microsoft Windows release approved by IT
MS Office, (Level approved by IT)
Symantic Antivirus
Adobe Reader
Dotnet
Flash player
Java
Springbrook PDF writer

Software Options:
Firefox
NERO
User Requirements

EMPLOYEE ACKNOWLEDGEMENT OF RECEIPT:

If you have any questions concerning this Policy or your obligations under it, please contact either your Supervisor or the IT department.

I ACKNOWLEDGE THAT I HAVE RECEIVED THE MONO COUNTY PC POLICY AND UNDERSTAND THAT I AM RESPONSIBLE FOR UNDERSTANDING AND ABIDING BY ITS CONTENTS.

Printed Employee Name: _____

Employee Signature: _____

Date: _____

The signed original of this page will be placed in the employee's personnel file. The employee will be given a copy of this page, along with a copy of the Mono County PC Policy.