OFFICE AUTOMATION SECURITY POLICY

SCOPE

The scope of this policy document includes all County owned or controlled PCs, laptops, servers, mini-computers, all data stored on those devices, all printouts or other media produced by those devices an all licensed software used on those devices.

OVERVIEW

This policy statement reflects accepted security controls taken from respected security and audit publications and adapted to Montgomery County's technical environment. These data security policies and standards have been developed to protect Montgomery County Government's electronic data asse from theft, destruction, and unauthorized modification or disclosure. The loss of these assets could be very costly and disruptive to the County government. In today's computing environment, security controls are a necessity. The citizens of this County will expect us to do what is prudent to protect the computing assets purchased with their tax dollars. Data is one of the most valuable assets of the Coun government. End-user computing dramatically increases the exposure for theft, corruption, loss, and misuse of County information resources since a significantly larger number of people have access to data and data security controls. A significant percent of direct access storage device capacity is install outside the Computer Center. Security is an issue that cuts across all computing and organizational tiers. The implementation of security policies and procedures requires cooperation among users, managers, information systems personnel, security and audit personnel and top management.

Access to all the County's computing and communication resources is to be controlled based on the needs of the County and used for official County business only. Connection and access to computing resources is controlled through unique user identification (user-ids) and authentication (passwords). Ea individual granted these privileges is responsible and accountable for work done under their unique identifier.

Computer users should be given a copy of the security policy by the management of their department when they are given a user-id.

Refer to the Internet Access Policy for additional information related to use of the Internet. This policy given to individuals receiving the authorized Internet connection software.

Much additional information is available on computer security for those wishing to do further research. Contact DIST security administration or reference the Internet for additional information.

RESPONSIBILITIES

The Department of Information Systems and Telecommunication (DIST), in accordance with Montgomery County code section 2-58D, is responsible for protecting the integrity of the telecommunications network backbone, for operation and maintenance and security administration of t "central" servers and for maintaining this policy statement.

Management in each department is responsible for ensuring that these computer security controls are enforced on the computing resources in their department and that appropriate training for computer us is provided.

The Local Area Network (LAN) administrator or Automated Systems Manager is responsible for implementing the computer security controls described in this document on the servers in their department. LAN administrators will contact DIST network management for allocation of IP addresses

As an owner of data or computing resources, a custodian of those assets or as a user, everyone is responsible for data security. Improper use of this information or of the access codes may result in a disciplinary action under the Montgomery County Ethics Law, Chapter 19A. Montgomery County Code or prosecution under Maryland Code. Article 27. Section 146.

PHYSICAL SECURITY

POLICY:

Access to file servers, individual PC's and minicomputers will be protected from unauthorized persons.

REQUIREMENTS & PROCEDURES:

Servers will be located in a closed area that may be secured by a locked door. If this is not currently feasible, system administrators will use keyboard locks or keyboard passwords and boot-protection to protect LAN servers from inadvertent or unauthorized keyboard access. When renovations are done, the LAN servers should be located in a closed area. If sensitive data is stored on individual PC's and these PC's are located in an open area, the same physical security considerations mentioned above for servers would apply. Periodically, an inventory of all computer hardware should be performed.

Wiring closets will be secured by a locked door to prevent unauthorized access to a sensitive area.

Any computer printouts or diskettes that are considered sensitive will be stored in a locked cabinet. There is a paper shredder currently in the judicial center for disposal of printouts if necessary. On-line viewing of sensitive material should be considered, where possible, as an alternative to printed reports.

Do not leave a PC unattended that is in an active session. Use keyboard locks or automatic screen blanking if planning to leave the PC for more than a few minutes without turning it off.

Use "power on" passwords when a PC is powered up. LAN administrators should keep a list of the power on passwords in a safe place in case they are forgotten.

Theft or physical abuse of County owned computer equipment is illegal. Report any occurrence of this to department management.

PASSWORD AND USER-ID ADMINISTRATION

POLICY:

Meaningful passwords will be used to protect access to County networked computer systems (LANs, mini-computers, PCs) and not shared with other individuals. Unused and default or installation user-ids will be disabled. Use of powerful user-ids such as those with system administrator attributes will be restricted.

REQUIREMENTS & PROCEDURES:

Passwords provide a basic first-level security for restricting access to computer resources. To protect County computer resources properly, passwords are required to access all networked computer systems. Passwords should be simple enough to memorize but unique enough to remain secret. Passwords will not be attached to a terminal or other public place where they are easily compromised. Passwords should not be associated with the current date or a person's name, hobby, or family. Good passwords are not found in the dictionary and contain numeric as well as alphabetic characters. Passwords will be at least six characters in length. Passwords will not be imbedded in user's automatic sign-on procedures unless approved by that department's management for procedures where it is required .

A maximum of thirty days between password change is required for LAN and mini-computer access. The change interval for power on passwords for PCs is at each department's discretion. Where possible, password change will be controlled automatically by security software. Passwords will be individually maintained to ensure confidentiality and individual accountability. Passwords will not be shared with others. If it becomes necessary to give your password to a technical person to fix a problem you are experiencing, the password should be changed once the problem is solved. An account will be suspended after no more than five invalid password attempts in a given day and remain suspended until an administrator can reactivate it. Passwords will not be reused for at least four monthly cycles. A user-id may be suspended after one year of non-use.

Access to computer resources will be terminated immediately for employees who leave County employment or when their responsibilities no longer require them to access those resources. Department coordinators are responsible for deleting or reassigning user-id's of people who have terminated or transferred out of the department. Computer system security will prevent a user-id from being logged on in two different places at the same time. Use of procedures that allow a user to login to a computer after their password has expired is discouraged (grace logins). If used, limit the number to two such occurrences. DIST Security Administration will be notified if changes to mainframe access rules are required due to deleted or reassigned user-id's. Just one user-id per computer platform will be assigned to an individual.

System privileges, such as supervisory or system administrator attributes are sensitive and are restricted to LAN or minicomputer system administrators and a backup. When the use of sensitive system privileges is necessary by others (for example, during an on-site visit by field service engineers), the privilege will be removed or the user-id disabled after the user is finished with the specific task.

Attempts to bypass security procedures to gain unauthorized access to computer resources is unacceptable and may result in disciplinary action.

PROTECTION OF SENSITIVE INFORMATION

POLICY:

Files containing sensitive information, and critical computer systems and applications will be protected from unauthorized access.

REQUIREMENTS & PROCEDURES:

Sensitive information includes criminal justice, payroll/personnel, client or patient information and any other data considered confidential by law or departmental policy. Sensitive information should not be stored on a PC unless PC security software has been installed on that PC. A PC that is used by more than one person or left on and unattended is a high risk environment in which to store sensitive information. Sensitive information should be stored on the mainframe or network server where better security is available to protect the integrity of this information. Access to this information will be restricted to those who have to use it. Examples of information that should be protected from unauthorized access include: word processing documents containing sensitive material, which should be locked (password protected); source code for programs, which should be protected using a source code management tool; databases, which should use all built-in security controls; and production files downloaded from the mainframe computer, which should be protected in a directory where limited access is permitted.

Sensitive information stored on computer diskettes, tapes or printout will be locked in a secure area when not in use and deleted or shredded when no longer needed.

The same level of security will be maintained across the various computer platforms (mainframe, mini, LAN or individual PC). If a sensitive file located on the mainframe computer is downloaded to an individual PC, that information on the PC will be protected from unauthorized access in anequivalent manner as it is on the mainframe.

Terminals or PC's should not be left unattended with the results of a query containing sensitive information displayed on the screen. If this is necessary, a screen locking feature that blanks the screen until the correct password is entered will be used. Sensitive printouts will not be left on an unattended printer.

Special care should be given for laptop or portable PC's. If possible. sensitive information should be stored on diskettes rather than the hard drive and in a separate secure location from the laptop. Some sensitive information may need to be encrypted in order to ensure adequate security. A power on password will be used. Remove the battery and power cord when traveling and store separately from the laptop. If the PC is lost or stolen, departmental and DIST Security Administration will be notified immediately.

If possible, unauthorized attempts to access sensitive information should be logged and kept for a period of at least thirty days.

Do not disclose userid's, passwords or other sensitive information to anyone without verifying their authorization to have this information.

BACKUP AND RECOVERY PROCEDURES

POLICY:

All mission-critical data on County computer resources will be backed up regularly and be recoverable.

REQUIREMENTS & PROCEDURES:

Data and files that are crucial to the department's operations will be backed up and the retention of at least the last three copies is highly recommended. The frequency of backups is commensurate with the frequency of change and the criticality of recovering the lost data in a timely manner. Some data may need to be backed up daily; monthly backups in other cases may be sufficient. When possible, backups should be automated.

Offsite storage facilities should be utilized for copies of backup files containing programs, data or transactions representing current County business that, if lost or destroyed, would be difficult to recreate. All backups should be retained a minimum of 90 days. Offsite storage facilities should also be utilized for files containing data with retention requirements imposed by County, federal or state government.

A detailed disaster recovery plan should be developed by each department that has a LAN or Mini-computer. This plan should detail procedures to follow in the event of the loss of computing hardware, software and data. A business continuity analysis should also be conducted that identifies the procedures that need to be in place in order to ensure that critical operations could continue in the event of a disaster which destroys their departmental computing capabilities. The conditions that warrant a disaster declaration and the persons responsible for this decision should be specified.

Contact the DIST Computing Information Center (CIC) if you need help in setting up backup and recovery procedures. Contact the DIST Computer Center for information on offsite storage procedures.

VIRUS CONTROL

POLICY:

All County owned servers and stand alone PC's will have up-to-date anti-virus software installed and activated. Users of County computers will be educated in computer virus prevention, recognition and steps to follow if a virus is suspected.

REQUIREMENTS & PROCEDURES:

Virus controls are necessary to prevent the spread of computer viruses to other computers in the network. Virus eradication can be very time consuming and result in the loss of service to the citizens of Montgomery County.

Software not purchased by the County (e.g. software from bulletin boards, software from home computers or any other computer or network), when allowed by County and department policy, will be checked for viruses before use. This includes diskettes, CD-ROMs and information downloaded from the Internet or other on-line services. Information downloaded to the hard drive will be checked immediately upon completion of the download. Diskettes and CD-ROMs received from other departments or agencies or from companies doing business with the County will be checked before use.

On a periodic basis, each department should certify that all server-based software and PC-based software is virus free. Contact CIC if information is needed on anti-virus software.

Use write protection whenever feasible.
- On 3.5 inch diskettes, move the write protect switch to the open position.
- On 5.25 inch diskettes, use write protect tabs.
- On hard disks, set the archive bit on executable files to "read only".

If you suspect a virus attack on your computer, the following steps should be taken immediately:
1. Call or page your department technical representative. If none is available call CIC.
2. Log off from and close all communications sessions (host, LAN, and modem-based).
3. Do not turn the system off until the help you called arrives and is aware of the suspicious symptoms.
4. Record recent activities to help track the infection. Make note of erratic system behavior leading up to the suspected virus attack. Make note of any diskettes that were loaded into the system or passed on to other users. Do not remove any diskettes from the area.
5. Place a large note on the on the PC indicating a virus infection to deter others from using the PC.

The LAN administrator should:
1. Make sure the PC is not communicating with other systems - disconnect the LAN cable.
2. Clean the virus off the PC and/or diskette.
3. Determine if the server or other PC's are affected and clean the virus off if found.
4. Document the incident for future reference.

The following list contains some of the common symptoms of viral infections:
1. Unusual characters on the screen.
2. Data inaccessible from hard disk.
3. Data or program files disappear.
4. Programs load or operate significantly slower than normal.
5. Unexplained change in file date and/or size.
6. Increased number of bad sectors seen using CHKDSK.
7. Decreased available RAM at boot-up seen using CHKDSK.
8. Unexplained system crashes or reboots.
9. The program tries an unauthorized write to a floppy or returns an "ABORT/RETRY" message.
10. A message is displayed on the screen stating that a virus is present.

DIAL-UP ACCESS TO COMPUTER RESOURCES

POLICY:

Dial-up access from a remote site to any Montgomery County computer resource will be approved by the employee's Department head or designee. The software and hardware necessary to utilize either "smart card" or "secure token" technology to authenticate dial-up access to County computer resources or encryption of the entire dial-up session is required. Unsuccessful access attempts will be logged if possible.

REQUIREMENTS & PROCEDURES:

Users or vendors who need dial-up access to any County computer resources will submit a request to the Mini or LAN administrator stating what the access is to be used for, how long the access is required, and approval from the responsible department official. Passwords and dial-back procedures are no longer considered adequate for secure dial-up access to County Computers. Contact DIST Security Administration for information on inexpensive and secure software to access Novell networks through a central communications server. Dial-back and password procedures are a minimum requirement until the "smart card" technology or encryption can be implemented. The list of authorized dial-up users will be reviewed periodically by the LAN or mini computer administrator to determine continued need for such access and accuracy of the list. If dial-up access is no longer required, that dial-up access will be terminated.

LAN and mini computer administrators will maintain a log of unsuccessful attempts to access County computers through dial-up lines. This log will be maintained at least thirty days. Default or unused user-id's will be disabled.

The following statement is wording approved by the County Attorney's Office that should be displayed to users when they access the computer from a remote location by telephone line:

"Warning: By using my access and identification codes, I understand and agree to the following: I have access to confidential information. I am responsible for the proper use and security of the information including printed reports. I am also responsible for the security for my access code to the system. I must not permit any other employee or individual the use of this data by borrowing my access code. Improper use of this information or of the access code may result in a disciplinary action under the Montgomery County ethics law, chapter 19A, Montgomery County code or prosecution under Maryland code, article 27, section 146."

User-ids will be automatically suspended after five invalid access attempts in a 24 hour period.

Encryption of any data that is sensitive is highly recommended if it is to be transmitted over public phone lines.

DIAL-OUT ACCESS TO REMOTE COMPUTER NETWORKS

POLICY:

Access to remote network services will be in accordance with the County-approved Internet Access Policy. Approval from the department management and DIST security administration will be obtained if a user requires a modem at their work station for remote access.

REQUIREMENTS & PROCEDURES:

Modems attached to PC's that are connected to a County network can be very risky and will not be authorized unless DIST-approved security measures are implemented. If remote access from a County owned PC using an attached modem is required, that PC will be disconnected from any LAN it happens to be connected to for the duration of the remote access session. Refer to the Internet Access Policy document.

ADHERENCE TO SOFTWARE COPYRIGHTS

POLICY:

No unauthorized copies of licensed software may be made or used.

REQUIREMENTS AND PROCEDURES:

It is a violation of copyright and trade secret laws and licensing agreements to make or use unauthorized copies of any licensed software. An inventory of all software should be made periodically to determine if the software is properly licensed. Automated tools such as software metering may be used to ensure compliance with license agreements. If illegal copies of software are found, they should be deleted from the system immediately or properly licensed.

Violation of this policy could result in fines to the County by the Software Publishing Association and disciplinary action to the employee.

EXCEPTIONS

POLICY:

Any exceptions to these procedures must be approved by the department management and DIST Security Administration.

REQUIREMENTS AND PROCEDURES:

Exceptions should be directed to DIST Security Administration by departmental management, in writing or via MEMO, for prompt consideration.

There are some older computer platforms in use in the County which lack the capability to implement some of the security procedures outlined in this document. Upgrades or replacements to these computer platforms should be purchased as soon as possible or sensitive information should be moved off these computers.