Montgomery County, Maryland

Computer Security Policy
(Interim)

Updated May, 2001
Department of Information Systems & Telecommunications

Table of Contents

1. SCOPE

The scope of this policy document includes all County owned or controlled computers (PCs, laptops, servers, mini-computers, mainframe), all data stored on those devices, all printouts or other media produced by those devices and all licensed software used on those devices. In addition, this Policy includes communications links to contractors and business partners and extensions of the County's computer network.

2. OVERVIEW

This is an interim security policy and will be updated. The policies outlined in this interim document will be in effect until they are superceded.

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 assets from theft, destruction, and unauthorized use, 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 County 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 installed 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). Each individual granted these privileges is responsible and accountable for work done under their unique identifier.

Computer users will be given a copy of the latest version of the Computer Security Policy and Internet, Intranet, & Electronic Mail Policy when they are given a user-id. Thereafter, County employees must adhere to the policies and are responsible for having the latest version of the policy. Refer to the *Internet, Intranet, & Electronic Mail Policy* for additional information related to use of the Internet.

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

3. RESPONSIBILITIES

All Montgomery County Government computing and communication hardware, software and data is considered to be "owned" by the Montgomery County Government.

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 the "enterprise" servers, mainframe and for maintaining this policy statement. DIST is responsible for insuring that computer connections between County departments and with other government agencies are accomplished securely and as authorized.

Management in each department is responsible for ensuring that these computer security controls are enforced on the computing resources in their department. These security controls will be enforced for employees as well as for contractors. Department management is responsible for providing pertinent information and notifying the DIST Security Office if a serious security breach occurs such as an intrusion, theft or damage of computing resources. The operation, maintenance and security of de-centralized computing resources is the responsibility of department management in accordance with security policy and other policies, as appropriate.

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 a user of data or computing resources or a custodian of those assets, 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.

4. PHYSICAL SECURITY

4.1 POLICY:

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

4.2 REQUIREMENTS & PROCEDURES:

Servers will be located in a closed area that will 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 will 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 will apply. Periodically, an inventory of all computer hardware will 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 [see Section 6] 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 will 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 password-enabled screensaver if planning to leave the PC for more than a few minutes without turning it off.

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

5. PASSWORD AND USER-ID ADMINISTRATION

5.1 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.

5.2 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 will 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 will not be associated with the current date or a person's name, hobby, or family. Good passwords are not found in the dictionary, contain numeric as well as alphabetic characters, and upper and lower case letters. 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. Use "power on" passwords when a PC is powered up if deemed appropriate based on the sensitivity of the data stored on the PC. LAN administrators will keep a list of the power on passwords in a locked cabinet in case they are forgotten.

A maximum of thirty days between password changes is required for server 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 will be changed immediately after 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 will 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. Access will also be terminated immediately for contractors no longer requiring access to County computer resources. Department coordinators are responsible for deleting user-id's of people who have terminated, transferred out of the department or no longer require computer access.

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. The DIST Security Office will be notified immediately 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 immediately 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 are unacceptable and may result in disciplinary action.

6. PROTECTION OF SENSITIVE INFORMATION

6.1 POLICY:

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

6.2 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 will 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 will be protected from unauthorized access include: word processing documents containing sensitive material, which can be locked (password protected); source code for programs, which can be protected using a source code management tool; databases, which can use built-in security controls; and production files downloaded from the mainframe or server, which can 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, reformatted 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 a equivalent manner as it is on the mainframe.

PC's and terminals will 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 will be given for laptop or portable PC's. If possible, sensitive information will 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. If the PC is lost or stolen, departmental security personnel and the DIST Security Office will be notified immediately, and a complete accounting of what was on that PC will be made.

If possible, unauthorized attempts to access sensitive information will be logged and kept for a period of at least one year. [See 10.2] This is information that may be used as evidence in a criminal proceeding and must be protected.

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

The following statement is wording approved by the County Attorney's Office that will be displayed to users before they are granted computer access:

WARNING: Unauthorized access is prohibited and punishable by law
[This warning banner will appear each and every time someone logs onto a County computer.]

7. BACKUP AND RECOVERY PROCEDURES

7.1 POLICY:

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

7.2 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 backup is to be 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 will be automated and take place during off-peak hours.

Offsite storage facilities will be utilized for copies of backup files containing programs, data or transactions representing current County business that, if lost or destroyed, would be difficult or impossible to recreate. All backups will be retained a minimum of four weeks and at least two copies will be kept in offsite storage. Longer retention periods should be considered based on business requirements. Offsite storage facilities will 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. This Plan should be practiced at least once a year; this practice will include restoring data from backup media to insure that restoration procedures are known and to verify the integrity of the backup media. 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.

8. SOFTWARE SECURITY UPGRADES

8.1 POLICY:

County computers will have all the current security patches and upgrades installed that are necessary to fix software security flaws.

8.2 REQUIREMENTS & PROCEDURES

Vendors publish patches and upgrades to their software when they discover security flaws that could allow computer security to be compromised. Employees responsible for computer resources will apply these updates to their application and operating system software. The DIST Security Office may provide information about enterprise software security issues and patches as available and appropriate.

9. VIRUS CONTROL

9.1 POLICY:

All County owned servers and 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.

9.2 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.

All those responsible for departmental computer resources will update those resources with anti-virus signatures on a monthly basis or more frequently and upgrade to the most current anti-virus release as it becomes available. Contact DIST's Computing Information center (CIC) if information is needed on anti-virus software. When DIST issues a security alert and specifies that virus signatures must be updated immediately, those responsible for departmental computer resources will comply.

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 will be taken immediately:

1. Call or page your department technical representative. If none is available call the Help Desk and follow their instructions.
2. 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.

3. Place a large note on the PC indicating a virus infection to deter others from using the PC.

The LAN administrator will:

1. Make sure the PC is not communicating with other systems - disconnect the LAN cable.
2. Contact the Help Desk and keep them informed of what you have found and your actions. Follow all Help Desk instructions.
3. Clean the virus off the PC and/or diskette.
4. Determine if the server or other PC's are affected and clean the virus off if found.
5. 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.

10. REMOTE ACCESS TO COUNTY COMPUTER RESOURCES

10.1 POLICY:

Access from a remote site to any Montgomery County computer resource will be approved by the employee's Department head or designee and by the DIST Security Office. Either "smart card", "secure token" or VPN technology will be used to authenticate remote access users to County computer resources. Unsuccessful access attempts will be logged if possible. All remote access systems used to access County computing resources will be approved by the DIST Security Office prior to purchase, installation or connecting to County resources.

10.2 REQUIREMENTS & PROCEDURES:

Employees or contractors who need remote access to any County computer resources will submit a request in writing to the DIST Security Office and the 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 remote access to County Computers (existing Rlink users are excepted from this statement until a conversion is announced). Contact the DIST Security Office for information on secure remote access options. The list of authorized remote access 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 remote access is no longer required, that access will be terminated.

LAN and mini computer administrators will maintain a log of unsuccessful attempts to access County computers through remote access lines. This log will be maintained for one year. Default or unused user-id's will be disabled.

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

11. ACCESS TO REMOTE COMPUTER NETWORKS FROM COUNTY COMPUTERS

11.1 POLICY:

Access to remote network services will be in accordance with the Internet, Intranet, & Electronic Mail Policy. Approval from the department management and the DIST Security Office will be obtained if a user requires a modem at their workstation for remote access.

11.2 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. Unauthorized modems attached to PC's that are connected to a County network are prohibited. If remote access from a County owned PC using an attached modem is required, that PC will be disconnected from all LANs for the duration of the remote access session. Refer to the Internet, Intranet, & Electronic Mail Policy document.

12. ADHERENCE TO SOFTWARE COPYRIGHTS

12.1 POLICY:

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

12.2 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 will 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 are to be deleted from the system immediately or properly licensed to protect the County from litigation. This discovery and deletion will be documented.

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

13. CONTRACTOR REMOTE ACCESS

13.1 POLICY:

All contractors will meet the same security requirements detailed in this and all other related County documents. The contractor will agree to, and is responsible for maintaining compliance with all County security policies. Virtual Private Network (VPN) and dial-up access (using info-key) are the current approved remote access methods.. The sponsoring Department head or designee and the DIST Security Office will approve the remote access request.

13.2 REQUIREMENTS AND PROCEDURES:

The department whose contractor requires remote access to the County's network will present a written justification to the DIST Security Office. All plans for establishing remote access will be approved by the DIST Security Office in advance of implementation. These plans will include at least the following:

Type of access
When and how long access will be required
Security procedures (how contractor access will be controlled)

All contractors requiring access will sign non-disclosure statements and agree to abide by all County security policies and procedures prior to receiving access.

14. EXTENDED NETWORKS

Extended Networks are permanent or semi-permanent physical extensions of the County's computer network to a non-County facility and used by non-County employees to access County computer resources.

14.1 POLICY:

All network extensions to a contractor or business partner facility will meet the same security requirements detailed in this and all other related County documents. The Contractor/Business Partner (C/BP) will agree to, and is responsible for maintaining compliance with all County security policies.

14.2 REQUIREMENTS AND PROCEDURES:

The Department requesting the extended network will present a written justification to the DIST Security Office for granting a C/BP access to the County's network from a remote location.

The C/BP will provide a secure link (e.g., T-1) between the C/BP site and the County's Computer Center. All plans for establishing a link will be approved by the DIST Security Office in advance of installation. These plans will include the following:

Type of connection
How long connection will be required
Hours of operation
Number and type of workstations and servers at remote location
Physical security plan
Security Procedures (including keeping all security systems up-to-date)
Anti-virus procedures (including keeping all anti-virus systems up-to-date)
Whether Internet access is required for any workstations
Training plan
The process of disconnecting the C/BP once the connection is no longer needed

The C/BP will maintain all security provisions, detailed in this security policy, while the remote location is connected to the County network. All employees that have access will sign non-disclosure statements, receive security training, and agree to abide by all County Security Policies and procedures (sign County security agreement), prior to receiving access. All training materials will be approved by the DIST Security Office in advance.

A list of employees with authorized access will be kept up to date and provided in a monthly report to the DIST Security Office. Requests for additional staff access will be approved by the DIST Security Office or County contract administrator prior to granting the access.

The C/BP will permit the DIST Security Office to inspect the remote location without notice, at any time. This may include technical scanning of the C/BP network segment and any system connected to it.

The C/BP network segment, defined as all workstations, servers, and network equipment connected to the County, will not also be connected to any other network (including the C/BP own internal network). Remote access to the C/BP network segment will NOT be permitted; dial-in or dial-out will not be allowed.

Failure to maintain full compliance with the County's security policies will result in immediate termination of the connection, and may be cause for cancellation of any contract between the County and the C/BP.

All material submissions mentioned above will be submitted by the Contractor / Business Partner to the County Department requesting the extended network, which will coordinate reviews and approvals with the DIST Security Office.

15. EXCEPTIONS

15.1 POLICY:

Exceptions to any of these policies or procedures must be approved by the department management and the DIST Security Office.

15.2 REQUIREMENTS AND PROCEDURES:

Exceptions will be directed to DIST Security Office by departmental management, in writing or via email, 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 will be purchased as soon as possible and until this occurs all sensitive information will be moved off these computers.