

SUBJECT: INFORMATION SYSTEMS ACCESS POLICY

EFFECTIVE
DATE: 11-18-11 (replaces 04-20-11)

APPROVED BY:

Reviewed (no changes): _____

Executive Director

POLICY

It is the policy of McIntosh Trail CSB to provide levels of security appropriate to the various classes of information and data held on file.

BACKGROUND/PURPOSE

The purpose of this policy is to maintain an adequate level of security to protect McIntosh Trail CSB's data and information systems from unauthorized access. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of McIntosh Trail CSB information systems.

IMPLEMENTATION/PROCEDURE

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

1. Who is Affected: This policy affects all employees of McIntosh Trail CSB, all contractors, consultants, temporary employees, and business partners. Employees who deliberately violate this policy will be subject to disciplinary action, up to and including termination.
2. Affected Systems: This policy applies to all information data, computer and communication systems owned or operated by McIntosh Trail CSB. Similarly, this policy applies to all platforms (operating systems) and all application systems.
3. Entity Authentication: Any user (remote or internal), accessing McIntosh Trail CSB networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes, but is not limited to:
 - A. Automatic logoff
 - B. An Unique user identifier
 - C. At least one of the following:
 - Biometric identification
 - Password
 - Personal identification number

SUBJECT: INFORMATION SYSTEMS ACCESS POLICY

EFFECTIVE
DATE: 11-18-11 (replaces 04-20-11)

APPROVED BY:

Reviewed (no changes): _____

Executive Director

IMPLEMENTATION/PROCEDURE (Continued):

1. Workstation Access Control System: All workstations (computers, laptops, or net books) used for McIntosh Trail CSB's business activity, no matter where they are located, must use an access control system approved by McIntosh Trail. In most cases, this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOS. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 2 hours). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.
2. Disclosure Notice: A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.
3. System Access Controls: Access controls will be applied to all computer-resident information based on its Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
4. Access Approval: System access will not be granted to any user without appropriate approval (FormDocs - Request for Technology Access). Management is to immediately notify the Security Officer and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.
5. Limiting User Access: McIntosh Trail CSB approved access controls, such as user log-on scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized.
6. Need-to-Know: Users will be granted access to information on a "need-to-know" basis. That is, users will only receive access to the minimum applications and privileges required to perform their jobs.
7. Compliance Statements: Users who access McIntosh Trail CSB information systems must read the compliance statement prior to issuance of a user-ID. A signature on request for access form indicates the user understands and agrees to abide by McIntosh Trail CSB policies and procedures related to computers, laptops, net books, air cards and information systems.

SUBJECT: INFORMATION SYSTEMS ACCESS POLICY

EFFECTIVE
DATE: 11-18-11 (replaces 04-20-11)

APPROVED BY:

Reviewed (no changes): _____

Executive Director

IMPLEMENTATION/PROCEDURE (Continued):

8. Audit Trails and Logging: Logging and auditing trails are based on the Data Classification of the systems.
9. Confidential Systems: Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:
 - a. Access time
 - b. User account
 - c. Method of access
 - d. All privileged commands must be traceable to specific user accounts
 1. In addition, logs of all inbound access into McIntosh Trail CSB internal network by systems outside of its defined network perimeter must be maintained.
 2. Audit trails for confidential systems should be backed up and stored in accordance with McIntosh Trail CSB backup and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports. Access for non-employees: Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use McIntosh Trail CSB computers or information systems unless the written approval of the Executive Director has first been obtained. Before any third party or business partner is given access to McIntosh Trail CSB computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.
 3. Unauthorized Access: Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of 'production data' must be restricted to 'production' applications.
 4. Remote Access: Remote access must conform at least minimally to all statutory requirements including, but not limited to, CMS and HIPAA.
 5. Conditions for use of computer equipment and software: Employees must read and agree to conditions contained in Attachment I and II.

Employees who are issued laptops and/or net books and air cards will be responsible for this equipment during the time of possession.

 - a. In the event the equipment is stolen, a police report should be filed documenting the McIntosh Trail CSB's equipment.
 - b. All equipment issued to employees by McIntosh Trail CSB should be returned at the time of termination/resignation/retirement. In the event the equipment is not returned, McIntosh Trail CSB reserves the right to withhold the employee's final annual leave check.

McIntosh Trail CSBCompliance, Confidentiality, and Non-Disclosure Agreement

Agency information that may include, but is not limited to, financial, consumer identifiable, employee identifiable, intellectual property, financially non-public, contractual, of a competitive advantage nature, and from any source or in any form (i.e. paper, magnetic or optical media, conversations, film, etc.), may be considered confidential. (Information confidentiality and integrity are to be preserved and its availability maintained.) The value and sensitivity of information is protected by law and by the strict policies of McIntosh Trail CSB. The intent of these laws and policies is to assure that confidential information will remain confidential through its use, a necessity to accomplish the agency's mission.

As a condition to receiving a computer User's Password and allowed access to a system, and/or being granted authorization to access any form of confidential information identified above, you must agree to comply with the following terms and conditions:

1. My User's Password is equivalent to my LEGAL SIGNATURE, and I will not disclose this code to anyone or allow anyone to access the system using my User's Password.
2. I am responsible and accountable for all entries made and all retrievals accessed under my User's Password, even if such action was made by me or by another due to my intentional or negligent act or omission. Any data available to me will be treated as confidential information.
3. I will not attempt to learn or use another's User's Password.
4. I will not access any on-line computer system using a User's Password other than my own.
5. I will not access or request any information I have no responsibilities for. In addition, I will not access any other confidential information, including personnel, billing, or private information.
6. If I have reason to believe that the confidentiality of my User Password has been compromised, I will notify McIntosh Trail CSB IT Department.
7. I will not disclose any confidential information unless required to do so in the official capacity of my employment or contract. I also understand that I have no right or ownership interest in any confidential information.
8. I will not leave a secured computer application unattended while signed on.
9. I will comply with all policies and procedures and other rules of McIntosh Trail CSB relating to confidentiality of information and User's Passwords.
10. I understand that my use of the system will be periodically monitored to ensure compliance with this agreement.
11. I agree not to use the information in any way detrimental to the organization and will keep all such information confidential.
12. I will not disclose protected health information or other information that is considered proprietary, sensitive, or confidential unless there is a need to know basis.
13. I will limit distribution of confidential information to only parties with a legitimate need in performance of the organization's mission.
14. I agree that disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by the authorized party.
15. This agreement shall survive the termination, expiration, or cancellation of this agreement.

CONDITIONS FOR USE OF COMPUTER AND SOFTWARE

Effective information management requires **PRIOR** approval, consent and authorization by the Information Technology (IT) Department of the following:

- ✓ Any and all changes to the computer hardware, including memory chips, cables, disk drives, printers, monitors, scanners, keyboards, mice, and/or modems. There should be no changes to your computer system unless authorized by or made by the IT Department personnel.
- ✓ Placement of or activation of any software or programs on the computer. Only those programs specifically approved and loaded by the IT Department are allowed on the agency's computer. No software or programs, including screen savers, should be loaded onto McIntosh Trail's computer system unless authorized by or loaded by the IT Department personnel.
- ✓ All computer equipment should remain in the same location as originally established unless proper authorization has been obtained from the IT Department for relocation of the equipment. The IT Department may either authorize relocation or assist in the relocation of all computer equipment.