

SUBJECT: COMPUTER PASSWORD POLICY

EFFECTIVE  
DATE: 05-21-03

APPROVED BY:

Reviewed (no changes):     03-31-05     01-20-10     Executive Director  
                                  11-06-07     03-24-11

---

POLICY

It is the policy of McIntosh Trail CSB to maintain security and accountability of employees' use of the agency's computer systems.

**PURPOSE:**

The purpose of this policy is to provide for the protection of McIntosh Trail CSB's information technology systems with secure password management. This policy pertains to all users and all levels of log-in access, directly or through an indirect source, to McIntosh Trail CSB's Information Technology environment. Information handled by McIntosh Trail CSB's systems must be adequately protected against unauthorized modification, disclosure, or destruction. Passwords are intended to prevent unauthorized access to McIntosh Trail CSB's systems and to ensure that users can access only the work they are authorized to perform. User IDs and passwords enable auditing and tracking of user activity. McIntosh Trail CSB reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

PROCEDURE

McIntosh Trail takes password security very seriously for a number of reasons, including:

1.     **Data Verification and Control:** Because of our consumer management system (Mitchell & McCormick) we process a great deal of information concerning our consumers. We must ensure the validity and correctness of this information and the manner in which it is entered into the system. In addition, we are required to maintain this information in a highly secure and confidential manner.
2.     **Break-ins:** All computer systems are connected to McIntosh Trail's network and the worldwide Internet. This makes access to multiple resources very easy and means that our systems are reachable from any computer on the Internet.
3.     **Impersonation/Identity Masking:** In order to insure that no one's password is used by another individual, we need the capacity to track who was using what computer at any given point in time.

SUBJECT: COMPUTER PASSWORD POLICY

EFFECTIVE  
DATE: 05-21-03

APPROVED BY:

Reviewed (no changes):     03-31-05     01-20-10     Executive Director  
                                  11-06-07     03-24-11

---

PROCEDURE (Continued)

4. For the reasons listed, McIntosh Trail CSB requires all staff to comply with a number of password security measures:
  1. All system users must have a signed user policy form on file before a password is assigned on McIntosh Trail's system. Once this form has been signed, the system administrator assigns a password and activates user name(s) on the appropriate systems.
  2. Passwords must withstand identification using standard hacking tools. Basic rules require that the password be: a) at least 4 characters long, b) not include or be based on your name or any word in any dictionary of any language, and c) include at least one letter (a through z) and one non-letter (1,2,3,4,5,6,7,8,9,0,!,@,\$,%, ^, etc.)
  3. You must not share your password with **anyone** under **any** circumstances. If misuse of computers is tracked to an individual's account, the individual will be assumed to have been the only person to know the password and may be subject to loss of computing privileges and/or other sanctions through McIntosh Trail's employee disciplinary actions, or law enforcement agencies.
  4. Passwords will be changed on a regular basis (normally every 90 days on most of our systems).
  5. Passwords are **not** to be written down anywhere.
  6. If an employee believes his or her password has been compromised, the employee must notify the IT Department as quickly as possible; the password will be changed.
  7. Users must comply with all rules established by the IT Department.
  8. Users will be locked out (disabled) after 5 failed attempts to log on within a 24-hour period. Employees with locked out accounts are required to communicate with the IT Department to negotiate re-establishment of their account.
  9. Offenses involving improper management by an employee of his/her own password, or the use of another's password, will result in disciplinary action, up to and including termination.