

1. ACCOUNT POLICIES

1.1 Account Holder's Responsibilities

- A. Account holders may use the TRECA computer systems for business-related activities only. Users are expected to report all potential misuse to their appropriate supervisor and/or to the TRECA Director or Systems Manager.
- B. Improper use includes, but is not limited to, the use of TRECA-owned and/or TRECA-operated computer systems and networks for the purpose of gaining unauthorized access to internal or external computer systems or accounts, for personal purposes, or for purposes of personal gain.

Examples of misuse could be transmitting offensive, harassing and/or devaluing statements, developing and transmitting inappropriate graphics, transmitting sexual or ethnic slurs or jokes, soliciting other employees, developing chain letters, communicating matters of private conviction or philosophy, permitting unauthorized access, etc.

- C. Account holders are responsible to safeguard their passwords, other access protocols, school district and TRECA information, in whatever form. This information is defined as any plans, ideas, or data that has not been approved for release to the general public. This could be technical data, business data, or employee data.

- D. Printed output that is considered confidential shall not be printed on any common printer. Instead, it must be printed in a secure area or some other restricted area, such as the employee's office.
- E. Account holders will ensure that their account is protected from unauthorized access. Passwords are the computer's first line of defense against unauthorized system access. All users should adhere to the following password controls:
 - (1) Passwords shall be non-meaningful terms. Passwords should not be of a common nature such as last name, job title, children's names, address, pet's names, etc.
 - (2) Passwords should not be displayed, divulged, or accessible to or shared with others. If there is any reason to suppose that a password has become known, it should be changed immediately.
 - (3) Passwords should never be written down, attached to the terminal, placed under the keyboard, or any other means which would allow for possible break-in.
 - (4) Users should be aware of the LAST LOGIN time of his/her account and report to the TRECA Data Center staff if it does not correspond with the last time they logged in.
 - (5) Users should not put passwords into command files.
- F. Users should notify the TRECA Data Center staff of any unauthorized access to their account when detected.
- G. Users should ensure their computers or terminals, when not in use, are properly logged off the system.

1.2 Account Management Policies

- A. Requests for new accounts must be submitted in writing using a TRECA Account Request Form. The approval process will include a written signature by either the user or the user's immediate supervisor. This signature represents the user's understanding and adherence to the policies contained in this document.
- B. Copies of the TRECA Account Request Form are available in electronic format and hardcopy formats. These can be obtained from TRECA's website or by contacting the TRECA Data Center.
- C. Account requests will be received Monday through Friday. The account request will be processed and available within three business days of receipt of a properly filled out form. The employee's immediate supervisor or district designated account coordinator will be contacted confirming the account creation. The account information will only be given to either the account holder or the district designated account coordinator. Passwords cannot be given to anyone else.
- D. All user accounts will be created with default privileges unless higher privileges are authorized by the appropriate district personnel and approved by TRECA.
- E. All account usernames on the state software system (currently known as TRECA0) will be setup with either the user's first name and last initial or the last name and first initial. If another user has the same first name and last initial, then the new account will contain the employee's first or last name and enough letters from the other name to form a unique username.

All account usernames on the eSIS software system (currently known as TRECA1) will be setup with an abbreviated district ID followed by the employee's first initial and last name.

- F. Passwords for new accounts will be initially set by the TRECA Data Center staff. All initial passwords will be randomized. It will be up to the employee to determine a proper password for subsequent changes. The initial password should be changed immediately by the user upon receipt.
- G. No GUEST accounts will be issued.
- H. For security reasons, each school district should immediately notify TRECA if an employee has been terminated or has left his/her organization. The accounts and files of terminated employees will be disabled immediately and the account and files will be deleted within five business days.
- I. Similarly for security reasons, each school district should notify TRECA when any account holder is placed on a leave of absence, short term or long term disability. That person's account must be completely disabled. The account can be reopened only at the request of the employee's immediate supervisor.
- J. Password controls for all accounts include the following:
 - 1. All district accounts are set to expire the password every 90 days. It is the user's responsibility to reset his/her own password. The password expiration will be 90 days from the time the password was last changed.
 - 2. All accounts will have a password minimum length of 8 characters. Up to 31 characters may be used. Letters, numbers, dollar signs and the underscore character may be used in a password.

3. If a password is lost or forgotten, the user's supervisor or the district designated account coordinator must contact the TRECA data center to establish a new one, which TRECA will then give to either the district designated account coordinator or the user. If the user contacts the TRECA data center directly to establish a new password, then the password can only be given to the district designated account coordinator. The Alpha computer stores passwords using a one way encryption algorithm. After they are encrypted, passwords cannot be returned to their original readable form. Since there is no method to look up a user's password, a new randomized password will be generated.
- K. Each district will be sent a list of active accounts once per year to verify the accounts within their district are current and accurate.