Network security, as well as physical workstation security, should be the concern of every DUSD technology user. Security issues on a single user's account/workstation can impact the system as a whole.

> *Security, by its very nature, makes accessing data, information and systems, difficult for non-authorized users.*

All DUSD network users should keep the following guidelines in mind:

- Never share your password. There is no valid reason to share your password with any other DUSD staff member or student.
- Never write passwords down on paper and leave them near your workstation.
- Never allow anyone to work on a computer, or DUSD data system, logged in as you. You are responsible for all activity performed under your login and can be held accountable for any data breaches, damage or access to confidential information.
- Substitute teachers are not allowed to use DUSD workstations under a staff member's login. The Tech Department will login a workstation, for a limited period of time, only for a site administrator or designated office personnel.
- Long-term substitutes will not be given access to a DUSD user's login. A board approved, long-term substitute will be given their own account and logins to the appropriate DUSD data systems.
- Students should never be allowed to work on a workstation under a staff member's login.
- Do not use your DUSD password on any outside service or web site.
- Do not respond to e-mail messages requesting you to update your DUSD password. The DUSD Technology department will never contact you by e-mail to update or get a new password. It will always be done over the phone or face-to-face.
- When a user is initially set up, workstations are configured for a maximum of 10 minutes of idle time, before automatically locking and forcing the user login again. The user should not change these settings.
- Never disable any security setting on DUSD workstations.
- Always use the most restrictive sharing functions on DUSD workstations, such as Bluetooth, file, printer and music, which still allow you to effectively perform your job duties.
- Any mobile device that accesses the DUSD network or services must be configured with a login passcode before being granted access to the network.
- Any walk-on Windows computer/mobile device that accesses the DUSD network must have an up-to-date antivirus subscription before being granted access to the network. This is checked annually by the Technology Department.

Every DUSD network user is responsible for network and workstation security. Any known violation of these guidelines will be reported to the user's site administrator and Superintendent. Employees found in violation of these guidelines will be disciplined up to and including termination.