

# Pittsburgh Public Schools Information Security Guidelines May 25, 2005

These guidelines are intended for use by all authorized account owners who have been provided user accounts by the School District of Pittsburgh to keep information secure.

## **Do:**

- know the District's *Password Policy*.
- inspect your data. If you suspect that someone has tampered with your files or the data contained in them, report it immediately to your supervisor or the Call Center.
- always insure your computer has up-to-date virus protection (no more than one week old).
- remember to back up data that is not centrally stored onto a local media such as CD-ROM or diskette. Don't expose this media to magnets or magnetic fields.
- label all CD's and diskettes and store them properly in a secured location.
- always log-off your system but leave it powered-on at the end of your workday. You may power-off the monitor.

## **Don't:**

- **ever** leave your active workstation unattended. If you walk away from your machine the CTRL-ALT-DEL option should always be used to lock the computer/server.
- copy, load or use borrowed, downloaded, or unsolicited software on District network/computer resources since these may contain computer viruses. The use of this software is in violation of the District's *Acceptable Use Policy* and may violate Federal copyright laws.
- store personal data on your computer. All work related sensitive data should be stored only on network shares.
- open pop-ups on your screen. These can lead to spy-ware being installed on your system without your knowledge.
- permit students to use any staff computer. This is a violation of the District's *Acceptable Use Policy*.
- provide copies of District data to anyone unless authorized by the Office of Information & Technology.