Policy No. 2164
Instruction

COMPUTER WORKSTATION SECURITY

The purpose of this policy is to provide direction for state employees in securing the Washington School for the Deaf computing workstations and network. All computers and workstations, PDA and WSD networks are affected.

Every workstation must meet the following configuration/usage standards:

- Employees shall use the operating system lock control mechanism whenever the system is left unattended. This is done at the computer through a key sequence Ctrl-Alt-Delete and Lock computer.
- Usernames and passwords are required to access the network. Passwords must be:
  - Changed when first assigned a login ID
  - Changed every 90 days
  - Be a minimum of 6 characters in length
  - Cannot be repeated within the last 3 password changes
- Employees are prohibited from displaying or sharing their password.
- After 5 unsuccessful login attempts, the account will be locked.
- WSD has the authority to perform audits on computers and devices connected to the network. The audits are performed to ensure the integrity, confidentiality, and availability of information resources; to ensure conformance to policy; to identify and investigate possible security threats; and to monitor user or system activity.
- Users are not allowed to install software on the network or workstations without prior authorization.
- Users are prohibited from downloading files from the internet without prior authorization.
- Computer workstations will operate with the minimum operating system configuration necessary to provide the necessary services.
- Unnecessary services will be disabled and required services will be hardened against intrusion.
- Any connection from WSD network to outside agencies must be approved by DIS. Connections will be allowed only with external networks that have been reviewed by DIS and found to have acceptable security controls. All connections approved will pass through DIS-approved firewalls. An example would be the Fortress system which gives access to the State of Washington intranet.
- All access to data on the network other than those within the scope of the job must get approval from WSD management.
- Backups are done on WSD servers only. Users should not store any

confidential or data they don't want lost on their workstation.

- Workstations utilizing the XP operating system get automatic updates and security patches.
- Anti-Virus software is installed and updated regularly to prevent attacks.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

PDA Personal Data Assistant
DIS Department of Information Services

Adoption Date: 12/09/04