

N. INFORMATION TECHNOLOGY – Data and Services/Security, Usage, and Recovery

The Board of Education recognizes the importance of establishing procedures for data and services, usage, security and recovery for computer resources for Palo Alto Unified School District (PAUSD).

The Department of Information Technology shall develop and maintain data security guidelines and standards to ensure that all student, personnel, financial or other vital data residing on PAUSD computer and network systems receive security protection from unauthorized use, access or distribution.

6/03

Administrative Procedures

I. To establish security procedures for Palo Alto Unified School District's (PAUSD's) computer systems.

A. Definitions

1. *The term "security" refers to the procedures that ensure only the authorized and intended parties have access to data and equipment.*
2. *The term "district resources" includes any services or other resources offered or owned by the PAUSD, including but are not limited to: e-mail, file servers, and eHomework, among other examples.*
3. *The term "computer system(s)" includes all hardware, software and data in the PAUSD computer network, including but not limited to mainframe computers, mini-computers, microcomputers, terminals, printers, communications devices, operating system software, networking software, other systems software, applications software and data.*
4. *The term "data system administrator" refers to the employee(s) designated in writing by the Superintendent as responsible for defining, controlling and scheduling appropriate data collection and entry into, and for approving the release of data from, designated computer system(s).*
5. *The term "level of access" defines the authorized read or update capability an individual has within the various computer systems.*
6. *The term "users" refers to all individuals authorized to access the computer system.*
7. *The term "program manager" refers to an employee who has been assigned the responsibility for an instructional/operational program within the PAUSD.*
8. *The term "terminal session" refers to the period of time during which the user of a computer system has access to an interactive system.*
9. *The term "unauthorized communication" refers to any communication that violates the Technology Use Policy or applicable local, state or federal laws.*
10. *The term "unauthorized site" refers to any physical site not part of the Palo Alto Unified School District.*

B. Applicability

This procedure applies to all computer systems in PAUSD.

C. Authorization/Revocation of Access Level – The Director of Technology by dated and signed writing may authorize, confirm or revoke access or levels of access of any identified individual to any designated computer system(s) or PAUSD's Secure Data Center(s), and by dated and signed writing may delegate or revoke delegation of such authority to any PAUSD employee (including but not limited to any identified principal or site administrator, data system administrator or program manager), subject to the following conditions and limitations and any additional conditions or limitations designated by the Director of Technology:

1. *Each and every PAUSD employee authorizing, confirming or revoking access or levels of access of any identified individual to any designated computer system(s) or PAUSD's Secure Data Center(s) shall promptly provide the Director of Technology with a copy of each writing dated and signed by that PAUSD employee authorizing, confirming, or revoking access or levels of access of any identified individual to any designated computer system(s) or PAUSD's Secure Data Center(s), including any conditions and limitations upon such access;*
2. *Any PAUSD employee exercising such authority shall exercise reasonable care to ensure that each individual authorized by that PAUSD employee to access any designated computer system(s) or PAUSD's Secure Data Center(s) follows all applicable laws, policies, rules and regulations regarding such access, including but not limited to PAUSD's Technology Use Policy, Student Records Policy, and these policies and procedures regarding Information Technology – Data and Services/Usage, Security and Recovery; and*

INSTRUCTION

3. *Each and every individual authorized access to any designated computer system(s) or PAUSD's Secure Data Center(s) shall exercise reasonable care to ensure that only authorized individuals are allowed access, including but not limited to checking whether any other individual is authorized before allowing access, by reference to list(s) posted by the Director of Technology or as otherwise directed by the Director of Technology.*

Upon the effective date of these policies and procedures, each principal and other site administrator shall promptly provide the Director of Technology with a written list identifying each individual having access and the level of access of such individual to the designated computer system(s) at their site, and for each such individual shall either confirm authority for such access in writing as provided above or advise such individual that these policies and procedures prohibit continued access and take all reasonable steps to ensure that such access does not continue.

- D. *Physical Security – Secure Data Center(s) are defined as an access controlled area or cabinet containing district servers or networking equipment.*
 1. *Entry into the Palo Alto Unified School District's Secure Data Center(s) shall be restricted to authorized individuals only.*
 2. *The Director of Technology will establish and enforce guidelines for maintaining the security of the Secure Data Center(s).*
- E. *Data Security – Industry standard methods of providing data security such as, but not limited to, passwords, firewalls, intrusion detection, encryption or authentication will be used as a means to prevent unauthorized use, access or distribution of PAUSD data.*
 1. *Authorization for Access*
 - a. *Data Network – Each data system administrator is responsible for identifying individuals who shall have access to the PAUSD network and determining the level of access an individual shall have.*
 - b. *Network Access – Methods of authentication for network access will be based upon the degree of the risk factor for network intrusion and compromise. Strong authentication is required for access to District resources from outside the PAUSD network. There are some PAUSD systems intended for certain public access; e.g., District Web site.*
 - c. *Termination of Access – School principals and program managers are responsible for maintaining a user's authorization log and for notifying the data system administrator when a user's authorization for system access is terminated.*
 - d. *User Awareness – The data system administrator shall be responsible for providing security awareness information to school principals and program managers for dissemination to students, faculties and staff.*
 2. *Passwords*
 - a. *Passwords for entry into the PAUSD network must be changed annually but shall be changed more frequently upon request of the data system administrator.*
 - b. *Written system passwords shall be secured in a locked repository.*
 - c. *The Director of Technology shall coordinate with data system administrators and program managers the exact time and date of password changes.*
 3. *User Responsibilities*
 - a. *Computer system users shall not reveal their passwords to anyone without prior approval of the user's program manager, data system administrator or the Director of Technology.*
 - b. *Users shall be provided with an initial password that may be changed at the user's discretion. User-created passwords should meet Password Standards and Guidelines for Issuing Employee Accounts and Services.*
 - c. *A terminal session shall not be left unattended or unsecured.*
 - d. *A terminal session shall be properly terminated at the end of the task or workday, whichever comes first.*
- F. *Unauthorized Use*
 1. *Prohibitions*
 - a. *The transmission of unauthorized communications on computer systems equipment or telecommunication devices is prohibited.*
 - b. *The use of computers for personal, commercial, political or private gain is strictly prohibited. Education Code 7054 (a) states that no school district funds, services, supplies, or equipment*

INSTRUCTION

shall be used for the purpose of urging the support or defeat of any ballot measure or candidate, including, but not limited to, any candidate for election to the governing board of the district. Employees shall use the system only for instructional purposes, school district business and incidental personal use.

- c. The downloading or installation of programs to the PAUSD computer systems without the written permission of the Director of Technology is prohibited.

2. Compromise or Incidents

- a. The data system administrator or program manager shall be immediately notified whenever passwords are compromised or incidents occur that may result in the compromise of passwords or data.
- b. The unauthorized use of computer system passwords by students or PAUSD employees shall result in disciplinary action as deemed appropriate.
- c. Violations of this regulation by persons not subject to PAUSD control or disciplinary measures that involve suspected criminal activity shall be referred to the Palo Alto Police Department.

3. Responsibility

- a. The Director of Technology shall be responsible for monitoring compliance with these procedures.

II. To provide guidelines and standards for the protection and security of the district's computer workstation systems and for the security of data and program files maintained on that hardware.

A. Definitions

1. The term "computer workstation(s)" includes all the hardware and software associated with any personal computer, desktop computer, or laptop computer used on the local-area network (LAN), wide-area network (WAN) of the Palo Alto Unified School District (PAUSD).
2. The term "network device(s)" includes the hardware and software that comprise the network infrastructure (LAN, WAN); e.g., routers, switches, etc.
3. The term "backup" refers to the process of copying files resident on computer disk(s) onto either magnetic tapes or additional disk(s).
4. The term "stand-alone" refers to a computer workstation not connected to any network.

B. Applicability

This procedure applies to all locations and to all applications using PAUSD computer workstations either in a stand-alone or networked environment.

C. Authorized Use

1. Only computer workstations owned by the District shall be used at the employee work location unless written authorization is obtained from the school principal and program manager.
2. Confidential student information shall not be transferred to personal computers.
3. Only employees authorized by the school principal and program manager shall access PAUSD computer workstations.
4. Only PAUSD employees authorized by the Director of Technology shall access PAUSD network devices.
5. The transport of any PAUSD computer workstation, network device or network configuration, program, or copy of software or data to an unauthorized site without the written approval of the Director of Technology is prohibited.

D. Hardware Protection

1. It is recommended that all PAUSD computer workstations have surge protectors or conditioned power.
2. Fileservers shall have uninterruptible power supplies ample for the given requirement.
3. A back up service is available upon request.
4. System software, operating systems and programs are duplicated and stored by the Department of Information Technology.
5. Backup media shall be kept in a secure physical location other than the location of the computer workstations.

INSTRUCTION

6. *All PAUSD computer workstations shall be located in an area that can be physically secured when the computer workstation is not in use.*
7. *No non-PAUSD computer workstation shall be connected to the PAUSD network without the prior approval of the school principal and program manager.*
8. *No network device shall be connected to the PAUSD network without the prior approval of the Director of Technology.*

E. Authorized Software and Data Protection

1. *Only software approved by the Director of Technology can be used on a PAUSD workstation. In all cases, software must have a proper license.*
2. *Software purchased by, or licensed by, the District shall not be copied except as authorized in a license agreement or by law.*
3. *All access to data that is recorded on PAUSD computer workstations and servers is governed and limited by existing policies and regulations for the protection of students, personnel, financial or other vital data information.*

F. Responsibilities

1. *Each school principal and program manager is responsible for ensuring the integrity and security of the data and the physical security of the hardware and software on PAUSD computer workstations within their respective school or program.*
2. *Each school principal and program manager is responsible for ensuring that each user who has a legitimate educational interest understands the confidentiality of data and the appropriate procedures for securing all data within their respective school or program.*
3. *Each user of a PAUSD computer workstation is responsible for ensuring the security of all their data that is recorded on the user's assigned computer workstation. Any computer that is used by a PAUSD employee must be left in a secure state.*
4. *School principals and program managers are responsible for ensuring that security violations within their respective school or program are reported to the Director of Technology.*
5. *The Department of Information Technology is responsible for maintaining the integrity and security of the PAUSD network.*
6. *Public or private contracted business associates shall have authorized access if they have signed a confidentiality agreement verifying that they will appropriately safeguard and maintain the integrity of data. Data is the property of PAUSD.*

6/03