Rules of Behavior for MSIN

Responsibilities

The MSIN (Migrant Student Information Network) is a WestEd information system operated for, and containing data owned by the California Department of Education and is to be used for official use only. Users must read, understand, and comply with these Rules of Behavior. Failure to comply with the MSIN Rules of Behavior may result in revocation of your MSIN account privileges, job action, and/or criminal prosecution.

Monitoring

This is a California Department of Education information system. System usage may be monitored, recorded, and subject to audit by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Unauthorized use of this system is prohibited and subject to criminal and civil penalties. System personnel may provide to law enforcement officials any potential evidence of crime found on any California Department of Education computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, RECORDING, and AUDIT.

MSIN Security Controls

The MSIN security controls have been implemented to protect the information processed and stored within the system. MSIN users are an integral part in ensuring the security controls for the site provide the intended level of protection. It is important to understand these security controls, especially those with which you directly interface. The sections below provide detail on some of those controls and the expectations for MSIN users.

MSIN security controls are designed to:

- Ensure only authorized users have access to the system;
- Ensure users are uniquely identified when using the system;
- Link actions taken within the system to a specific user;
- Ensure users only have access to perform the actions required by their position;
- Ensure MSIN information is not inappropriately released; and
- Ensure the MSIN is available to users when needed.

Examples of security controls deployed within MSIN include:

- Automated Session Timeout –Users are automatically logged out of the MSIN after 20 minutes of inactivity. This helps ensure unauthorized users do not gain access to the system.
- Role-Based Access Control –User names are assigned a specific role within the MSIN. This role corresponds to the user's job function and restricts access to certain MSIN capabilities.
- Audit Logging –Actions taken within the MSIN are captured in log files to help identify unauthorized access and enforce accountability within the system.
- Incident Response –If a user suspects their user name has been subject to unauthorized use, contact the MSIN Help Desk immediately.
- Communication Protection –Traffic between a user's web browser and the MSIN servers is encrypted to protect it during transmission.

Protection of MSIN Information

You are required to protect MSIN information in any form. This includes information contained on printed reports, data downloaded onto computers and computer media (e.g., diskettes, tapes, compact discs, thumb drives, etc.), or any other format. In order to ensure protection of MSIN information, you should observe the following rules:

- Log out of MSIN if you are going to be away from your computer for longer than fifteen minutes.
- Lock your computer before you leave it unattended by using the Ctrl+Alt+Delete key sequence when leaving your seat.
- Media (including reports) containing MSIN information must be placed in a locked location prior to being left unattended during non-business hours.
- Store media containing MSIN information in a locked container (e.g. desk drawer) during non-business hours.
- Store digital information in an encrypted format, using a FIPS 140-2 validated solution, when the information will be placed on portable devices and when the information will traverse the Internet or other public networks.
- Media containing MSIN information should be properly cleansed or destroyed.
    - Shred paper media and compact discs prior to disposal.
    - Diskettes and other magnetic media should be cleansed using appropriate software or a magnetic field with sufficient strength so as to make the information unreadable. (To the United States Department of Defense standard 5220.22-M)
        - Note that simply deleting files from magnetic media does not remove the information from the media.
- If the access which you have been granted within MSIN is more than required to fulfill your job duties, it should be reported to appropriate personnel.
- Protected data should not be emailed. If dissemination is required, a secure method should be used following the California Department of Education requirements.

- Do not disclose MSIN information to any individual without a “need-to-know” for the information in the course of their business.

Redisclosure and Use of Third Parties Forbidden

MSIN and the data contained within the system is the property of the California Department of Education. WestEd is the authorized contractor charged with developing, maintaining, securing, storing, and overseeing MSIN data collection activities. As such, access to MSIN is restricted to only those who have been given explicit access to the system. Login credentials, system code, and data contained within MSIN shall not be disclosed to any third parties without explicit permission from CDE and WestEd. Prohibited uses include but are not limited to:

- Sharing login credentials (passwords and user ID’s)
- Connecting MSIN to 3rd party technology, applications, or systems
- Releasing MSIN data to 3rd parties for analysis, storage, or other processing

Privacy Statement

The MSIN is a WestEd information system operated for and containing data owned by the California Department of Education, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this information system may subject violators to criminal, civil, and/or administrative action.

This system contains personal information protected by federal and California state privacy laws including, but not limited to: Family Educational Rights and Privacy act of 1984 (20 U.S.C.Sec. 1232g), COPPA, California Education Code Sections 49069 to 49079, and California Information Security Practices Guide for State Agencies (2008). Violations to the provisions of the privacy laws listed above may subject the offender to criminal penalties.