# Migrant Student Information Exchange (MSIX)

# Rules of Behavior

### Rules of Behavior

## Responsibilities

The Migrant Student Information Exchange (MSIX) is a Department of Education (ED) information system 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 MSIX Rules of Behavior may result in revocation of your MSIX account privileges, job action, or criminal prosecution.

MSIX users must complete a basic security awareness training course prior to being granted access to the system. The security topics addressed in this document provide the required security awareness content, so it is important that you read through this entire text. Users must also complete annual security awareness refresher training. MSIX will prompt you to reread the Rules of Behavior annually (or more often due to changes in the system or regulations) to meet this requirement.

**MSIX users are responsible for notifying their MSIX User Administrator when they no longer require access to MSIX. This may occur when a user gets new responsibilities that do not include a need to access MSIX or when the user gets another job or position.**

## Monitoring

This is a Department of Education computer 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 Department of Education computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, RECORDING, and AUDIT.

## MSIX Security Controls

MSIX security controls have been implemented to protect the information processed and stored within the system. MSIX users are an integral part in ensuring the MSIX security controls 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 MSIX users.

MSIX security controls are designed to:

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

Examples of security controls deployed within MSIX include:

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

The sections below describe several other security controls in place within MSIX. It is important that you understand and comply with these controls to ensure the MSIX security is maintained.

## User Credentials

User credentials are the mechanism by which MSIX identifies and verifies users. These are your user id and password. User ids uniquely identify each MSIX user and allow the MSIX System Administrators to attribute actions taken within the system to a specific user. This tracking is important in enforcing accountability within the system. Passwords are used by MSIX to verify a user’s identity. It is important for you to comply with the following rules governing user credentials:

- Protect your logon credentials at all times.
- Never share your user id and/or password with anyone else. You are responsible for all actions taken with your user credentials.
- Your passwords must:
  - Be changed upon initial login to MSIX;
  - Contain at least eight (8) characters;
  - Contain a mix of letters (upper and lower case), numbers, and special characters (#, @, etc.);
  - Be changed at least every ninety (90) days; and
  - Not reuse your previous six (6) passwords.
- Do not write your password down or keep it in an area where it can be easily discovered.
- Avoid using the “remember password” feature.
- User accounts are disabled after three (3) consecutive invalid attempts are made to supply a password.
- Reinstatement of a disabled user account can only be reinstated by a Help Desk technician or a system administrator.

## Protection of MSIX Information

You are required to protect MSIX 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 MSIX information, you should observe the following rules:

- Log out of MSIX if you are going to be away from your computer for longer than fifteen minutes.
- Log out of MSIX or lock your computer before you leave it unattended by using the < Ctrl > < Alt > < Delete > key sequence when leaving your seat.
- Media (including reports) containing MSIX information should be removed from your desktops during non-business hours.
- Store media containing MSIX information in a locked container (e.g. desk drawer) during non-business hours.

- Store digital information in an encrypted format where technically possible.
- Media containing MSIX 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.
        - Note that simply deleting files from magnetic media does not remove the information from the media.
        - Media containing encrypted information can be excluded from the cleansing process, although it is recommended.
- If the access which you have been granted within MSIX is more than required to fulfill your job duties, it should be reported to appropriate personnel.
- Do not disclose MSIX information to any individual without a "need-to-know" for the information in the course of their business.

## Other Security Considerations

This section describes some additional security items of which you should be aware.

- <u>Incident Response</u> - If you suspect or detect a security violation in MSIX, contact the MSIX Help Desk immediately. For example, if you suspect someone may have used your user id to log in to MSIX, you should contact the MSIX Help Desk. Other warning signs that MSIX may have been compromised include, but are not limited to: inappropriate images or text on the web pages, data formats that are not what is expected, missing data, or MSIX is not available. While these may not be attributed to a compromise, it is better to have it checked out and be sure than to take no action.
- <u>Shoulder Surfing</u> - Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. An example of shoulder surfing is when a person looks over someone else's shoulder while they are entering a password for a system to covertly acquire that password. To protect against this type of attack, slouch over your keyboard slightly when keying in your password to block the view of a possible onlooker.
- <u>Social Engineering</u> - Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. For example, a typical social engineering attack scenario is a hacker posing as an authorized user calling a system help desk posing as that user. The hacker, through trickery, coercion, or simply being nice coaxes the help desk technician into providing the login credentials for the

user he is claiming to be. The hacker then gains unauthorized access to the system using an authorized user's credentials.

The example above is one example of a social engineering technique. Another is when a hacker calls a user at random and pretends to be a help desk technician. Under the guise of purportedly fixing a problem, the hacker requests the user's login credentials. If provided, the user has unwittingly provided system access to an unauthorized person.

To defeat social engineering simply question anything that doesn't make sense to you. For example, a help desk technician should never ask a user for their login credentials to resolve a problem. If you receive a call from someone and you are not sure who they are, ask for a callback number. Hang up the phone and call back to the number provided. Hackers will typically provide a bogus number. Ask questions. If the answers you receive do not make sense, end the call and report the incident to your local security organization.

- Faxing - When faxing MSIX information, call the recipient of the fax and let them know it is coming. Ask them to go to the fax machine so they can pull it off right away so any sensitive information is not left lying around the office.
- Virus Scanning - Scan documents or files downloaded to your computer from the Internet for viruses and other malicious code. Virus scanning software should also be used on email attachments.