MIGRANT STUDENT INFORMATION EXCHANGE (MSIX)

Cybersecurity and Account Management Webinar

FEBRUARY 24, 2022

Deloitte

msix

PRIVACY REMINDER

The Migrant Student Information Exchange (MSIX) contains real and sensitive student data that **should not be shared** with those who do not need it.

Protecting a child's Personally Identifiable Information (PII) is paramount when using MSIX.

If there is a PII incident,
contact the MSIX Help Desk immediately.

msix

Agenda

1. MSIX Overview
2. Cybersecurity and Privacy Awareness Training
3. MSIX Account Management Reminders

MSIX Overview

MSIX is a web-based application that links State migrant systems to produce a single Consolidated Student Record containing the Migrant Education Program (MEP) minimum data elements (MDEs) to not only analyze national migrant trends, but also facilitate:

Enrollment

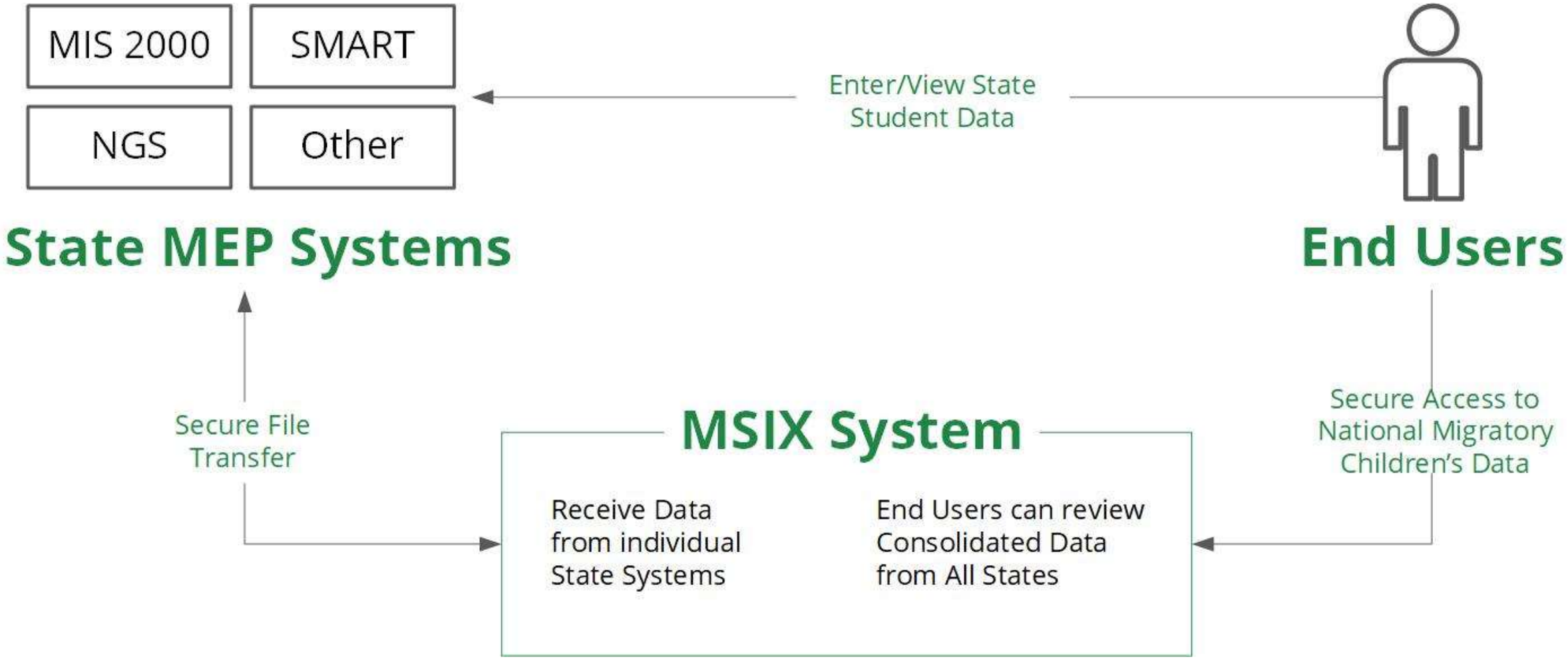
Placement

Credit Accrual

MEP Participation

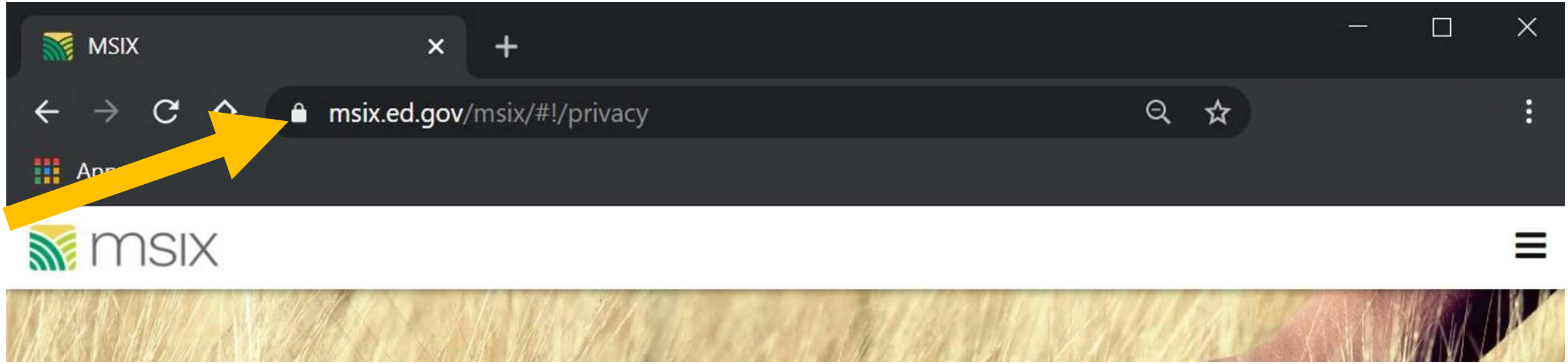
msix

MSIX Overview | *System Architecture*



msix

MSIX Overview | *Secure Access*



msix

Cybersecurity and Privacy Awareness Training

Federal and U.S. Department of Education Cybersecurity References

Federal Government

- Federal Information System Modernization Act of 2014 (FISMA)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Revision 5

Department of Education

- OCIO: 3-112 Cybersecurity Policy

MSIX Specific

- MSIX System Security Plan
- MSIX Privacy Impact Assessment
- MSIX System of Record Notice
- Interconnection Security Agreements
- Memoranda of Understanding
- MSIX Rules of Behavior

msix

Cybercrime Statistics

1. **Email threats rose by more than 64% during 2020**

With employees around the world working remotely, more sharing of sensitive business information has migrated from conference room white boards and face-to-face conversations. This swell of digital activity has presented cybercriminals with numerous new openings for social engineering attacks.

2. **60% of business endured a ransomware attack last year**

The (ITRC) reported in 2021 that cybercriminals remain less invested in taking large amounts of personal information instead manipulating poor consumer behaviors to perpetrate identity-related crimes against businesses using stolen credentials, such as logins and passwords. Criminals then utilize these stolen logins and passwords to perpetrate ransomware and phishing attacks.

3. **There is a cyber-attack once every 39 seconds**

According to a study from the University of Maryland, a typical computer is attacked in one way or another every 39 seconds. This could come in the form of a direct hacking attempt, a phishing attempt, or some other version of spam meant to infect your computer with malware.

msix

Avoid a Social Engineering Attack

DO

- Be suspicious of unsolicited phone calls, visits, or email messages from people asking about employees, computer systems, or internal information
- Try to verify the identity of any unknown person who claims to be from a legitimate organization
- Remember legitimate personnel will NEVER ask you for your password

DON'T

- Give your passwords to anyone
- Enter your credentials into a website accessed by clicking a link in an email message
- Allow an unknown individual remote access to your computer in response to an unsolicited telephone call or onscreen pop-up message

msix

Email Security Best Practices

1. Do not open unexpected attachments even if you know the sender
2. Do not click on suspicious links within emails
3. Install and update anti-virus software on all devices
4. Learn how to recognize phishing
    - Messages that contain threats to shutdown accounts or devices
    - Requests for personal information (passwords or Social Security Numbers)
    - Words like “Urgent”
    - Forged email addresses
    - Poor writing or bad grammar
5. Don’t give your email address to sites you don’t trust
6. Report suspicious emails to your IT Department

msix

General Security - PA

Required Training

- PA requires all staff to attend the annual OME Security Webinar
- PA has developed a comprehensive Security Webinar and updates it annually based on new material provided by OME or annually at our State Conference and other times as needed

New Staff

- New staff must review the material in this webinar with a data staff member when hired and prior to obtaining an MSIX login
- New staff must then attend the next formal security presentation when it is available

Best Practices

- Staff are constantly reminded of best practices related to securing data
- Staff are trained in FERPA and that only those with an educational need may have access to student records (and only for those students they have need to access)

msix

Annual Required Trainings

In New York, security training is required for all staff on an annual basis. Staff are trained on the **Three "C"s of Security**

Secure Conduct
Thinking secure when interacting with student data

Secure Computers
Ensuring all devices accessing student data are properly secured

Secure Communications
Utilizing secure methods to connect and send data over the internet

msix

Secure Conduct

In New York, staff are trained on how to think secure when using any technology. Some techniques we emphasize are:

- Considering **FERPA** whenever student data is requested
- Spotting a phishing scam via emails and phone calls
- Noticing attempts at social engineering
- Never sharing account credentials with anyone else
- Using Multi-Factor Authentication (MFA) whenever possible

msix

Understanding PII, SPII, and PHI

PII

Personally Identifiable Information

Any information about an individual that you can be used to distinguish or trace an individual's identity alone or when combined with other information linked or linkable to the specific individual.

SPII

Sensitive Personally Identifiable Information

PII is considered SPII if its improper release could result in harm, embarrassment, inconvenience, or unfairness to the individual whose name or identity is linked to the information.

PHI

Protected Health Information

PHI is any personal health information that can potentially identify an individual, that was created, used, or disclosed while providing healthcare services, whether it was a diagnosis or treatment.

Note: MSIX does contain PII but not SPII or PHI. Please do not input a child's SPII or PHI into MSIX via file submission or using the correspondence feature.

msix

Sharing PII

Stop and think:

- Before sharing PII/SPII, ask yourself who you are sending it to and whether they "need to know" the information.
- To prevent accidentally sending information to the wrong person, address your message carefully. Make sure you select the correct recipient.
- **Follow your State laws** to ensure you are using approved transmission methods and required protections (e.g., encryption).
- Never download or store PII on personally-owned equipment.
- Do not upload PII to an unauthorized online storage site (e.g., Dropbox, wikis, etc.).
- PII should never be accessed from public computers or kiosks found in hotel business centers or airports.

TIP! **Do not send PII to the Help Desk without first speaking with a Help Desk representative.**

msix

PII in PA

- PII, security/phishing, data breaches, strong passwords are explained
- All computers used by staff working with PII are encrypted
- Staff are reminded to never tape passwords to computers/keep with or near the computer or share them with others
- Staff must lock computers whenever not at the computer and also warned about "shoulder surfing"
- Staff must never email any PII unless it is encrypted and then the password must be sent via a different method (telephone/text/in person) and NOT simply via a separate email
- Staff are reminded that paper records and external devices such as flash drives must also be secured
- Staff are strongly reminded of THEIR personal role in all of this

msix

Maintain Situational Awareness

Situational awareness is always being aware of your surroundings. It can prevent unauthorized access to sensitive information including PII.

Constantly remind yourself to stay aware, especially when you are in non-private areas (e.g., hallways, elevators, or open office spaces) or off-duty (e.g., during lunch, on coffee breaks, while on vacation or traveling, shopping, talking on the phone, etc.).

- **Sensitive information should only be discussed in private, controlled areas**
- **Be aware of your surroundings and the people around you**
- **Take care when reading or viewing sensitive information outside of the office. Unauthorized individuals may be able to reach or view the information as well**
- **Be discreet when retrieving messages from smartphones and other media. Don't include sensitive information in voicemail messages**
- **Do not share sensitive information with anyone else unless he or she has a work-related need to know**

msix

Digital Assistants: Best Practices

Digital assistants, like Siri on iPhones and iPads as well as smart speakers such as Amazon Echo and Google Home, are **configured to constantly listen for commands.**

Turn off your digital assistant when participating in conference calls.

msix

Home Wireless Networks: Best Practices

Keep it Secure

- Secure your Wi-Fi network and your digital devices by **changing the factory-set default password and username**.

Understand the Security Features

- **Do not use Wired Equivalent Privacy** (WEP), which can be hacked in minutes.

Hide the Identity

- **Turn off the identifier-broadcasting** feature of your router. **Create a guest wireless network** just for your laptop.

Connect to VPN

- **Connect** immediately after logging into your laptop

msix

Public Wireless Networks: Best Practices

Use Caution

- **Be wary** of connecting to any network that is identified as "Free Wi-Fi."

Connect to VPN

- Ensure VPN is connected as soon as possible and **limit your activity to web browsing**. **Avoid accessing any services that require entering credentials** (e.g., username and password) or personal information.

Use Hotspot

- Another safer option for accessing the internet is to **use your phone's hotspot.**

msix

Secure Computers

In New York, work devices that may access student data are configured to be as secure as possible

- Full device encryption safeguards data on the computer
- Antivirus protects against malicious programs
- Secure cloud storage platforms prevent data loss

Secure Communications

In New York, all communications are required to be done through secure channels

- **VPNs** are required for public WiFi, and **mobile hotspots** are encouraged instead when possible
- Student data may never be sent as plaintext over email and instead must always be encrypted or sent through a more secure platform
- Staff are trained on using **separation of mediums** when sharing encryption keys, so that an encrypted file and its password are never both be sent over email

msix

MSIX Password Policy

1. Between **12 and 20 characters**.
2. Include at least one character from each of the four main character classes:
    a. Uppercase letters [A-Z]
    b. Lowercase letters [a-z]
    c. Non-alphanumeric special characters [!,@,#, etc.]
    d. Numbers [0-9]
3. Users may not re-use any of their **previous 24 passwords**.
4. Passwords must be changed **after 90 days** of use.
5. Accounts will be locked after **three (3) consecutive login attempts**

msix

Accessing MSIX

New users work with their User Administrator to complete the **User Access Application,** Cybersecurity Training, and acknowledge the MSIX Rules of Behavior to obtain access to MSIX.

Status	Time Frame/Conditions	Password Reset
Active	**Day 1 – 90 days** after account activation or password reset.	1. Initiate Password Reset using "Forgot Your Password?" on the MSIX Login Page. 2. Answer Challenge Questions to obtain a One-Time Password (OTP) via email. 3. Use the OTP to login to MSIX and reset your password.
Locked	Incorrect username/password combination entered 3 times.	1. Initiate Password Reset using "Forgot Your Password?" on the MSIX Login Page. 2. Answer Challenge Questions to obtain a One-Time Password (OTP) via email. 3. Use the OTP to login to MSIX and reset your password.
Expired	**91 days – 120 days** after account activation or password reset.	1. Initiate Password Reset using "Forgot Your Password?" on the MSIX Login Page. 2. Answer Challenge Questions to obtain a One-Time Password (OTP) via email. 3. Use the OTP to login to MSIX and reset your password.
Disabled	**121 days** after account activation or password reset or manually disabled at any time.	Contact User Administrator.
Deactivated	**1 year** after account disablement or manually deactivated at any time. *This is a permanent action.*	Contact User Administrator to complete your State's account application process to re-establish access.

Self-Managed Password Reset Process

1. Click on the "Forgot Your Password?" link on the MSIX login page and enter your username.
2. Answer **three of your five challenge questions** to receive an email with your one-time password.
3. Use your username and the one-time password from the email to log into MSIX.
4. Confirm your challenge questions and responses.
5. Now, you can set your **new password**!
6. Remember, you can view and edit the answers to your challenge questions on the "My Account" page at any time.

msix

MSIX Usage - PA

- PA is a Regional Based Program
- All PA staff who work with children/families must have MSIX accounts and usage is monitored and recorded in our database
- Many attempts have been made to have district staff obtain accounts
  - Most district staff rely on the MEP, and our MEP staff are terrific at building relationships with schools
  - PA continues to encourage staff outside of the MEP to obtain accounts. There has been little success primarily because they rely on the Regional MEP staff who do a great job in working with them.
  - Districts in PA require formal transcripts and immunization records.

msix

Annual MSIX Account Applications

In New York, access to MSIX must be reapplied for annually using a prepared form. This helps ensure that no disused account gets overlooked and that only the individuals still requiring access to MSIX can continue to do so.

Completion of our annual security training is required for approval.


NEW YORK STATE
MIGRANT EDUCATION PROGRAM

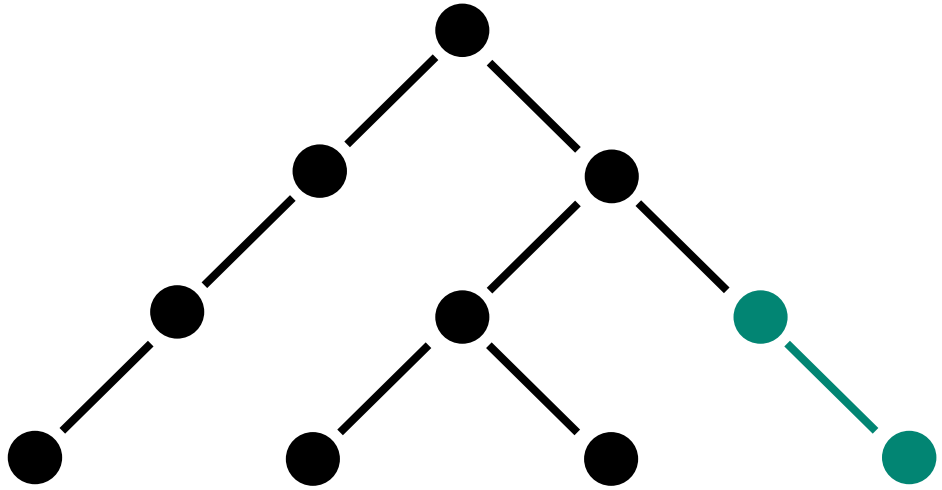
MSIX USER ACCOUNTS - NEW ACCOUNT CREATION FORM

msix

Principle of Least Privilege

This is the principle of granting the least amount of access necessary to perform one's job duties. Following the Principle of Least Privilege better safeguards the system data against possible compromise.

In New York, student data is only granted to the employees who work with those students



msix

Password Managers & Passphrases

In New York, the usage of password management software and strong passphrases is encouraged

Passphrases

- A phrase or short sentence used in place of a password that is usually easier for the user to remember and more difficult for an attacker to guess

Password Managers

- A program that generates and stores passwords in a secure vault

msix

User Administrator Responsibilities

1. **Reset passwords** for disabled accounts.
2. **Initiating a password reset** for an active, locked, or expired account will give the user an opportunity to reset their challenge questions.
3. **Create new accounts**
    - New users will receive **two** emails: one with new username and a second with a one-time password.
    - After logging in using the one-time password, new users will be required to set up their challenge questions and set their password.
4. **Disable or Deactivate accounts** for MSIX users who no longer have a need to access the system.

TIP! **Use the Account List Report to review user accounts within your State.**

msix

Thank You!

FEBRUARY 24, 2022

msix