# Migrant Student Information Exchange (MSIX) Security, Privacy and Account Management Webinar

**Deloitte Consulting LLP.**
**February 22, 2018**


**Maria Hishikawa – MSIX Technical Lead**
**Sarah Storms – MSIX Contractor Security**

# Introductions

*This Webinar is being recorded.*

- **Agenda:**
  - MSIX Account Management Improvements/Changes
  - Part 1: Security and Privacy Awareness Training for All MSIX Users
  - Part 2: User Administration Role-Based Training for User Administrators and State Migrant Education Program (MEP) Directors

***You are invited to attend the Part(s) that pertains to your role within MSIX***.

# Account Management Improvements/Changes

- Shorter-Term
  - Updated Account Application with Intended Use section
  - Automatic disabling of unused accounts

- Longer-Term
  - Streamlined new user application and registration
  - Self-service account/password management
  - Enhanced user login experience
  - Enhanced security for privileged users

# Part 1: 2018 Security and Privacy Awareness Training

Objectives:

- MSIX Users will:
  - Understand laws, policies and procedures that govern MSIX Accounts Management
  - Understand current cyber security threats
  - Understand accounts management terminology
  - Understand Do's and Don'ts of accounts management
  - Identify suspicious email messages
  - Understand proper handling of Privacy information and Personal Identifiable Information (PII) while using MSIX

# Federal and ED Cybersecurity References

## Federal Government Wide

- Federal Information System Modernization Act of 2014 (FISMA)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Revision 4

## US Department of Education

- US Department of Education (ED) Office of Chief Information Officer (OCIO) OCIO-01 Information Assurance / Cybersecurity Policy (Jan. 2017)

## MSIX Specific

- MSIX System Security Plan
- MSIX Privacy Impact Assessment

# Cyber Security Threats in the News

- **EQUIFAX Breach**
- **OPM Hacked**
- **YAHOO Accounts Stolen**
- **ANTHEM PII Stolen**

**In 2016:**

- 81% of breaches leveraged stolen or weak passwords
- 43% were social engineering attacks
- 75% perpetrated by outsiders
- 25% involved internal actors
- 27% of breaches were discovered by third parties

**Real Threats to MSIX**

- Key Logger
- Email Phishing

# Cybersecurity Terminology

- **Identification** - a user claims or professes an identity with a username, a process ID, a smart card, or anything else that can uniquely identify a subject
- **Authentication** – a user provides appropriate credentials to prove an identity
  - Something you have: smartcard or RSA key
  - Something you know: password
  - Something you are: biometric (fingerprint)
- **Authorization** – a user is granted access to a system
- **Role-Based Access Control** – a user is granted access to resources based on his role
- **Separation of Duties** –more than one person is responsible for a task
- **Least Privilege** – user's role matches assigned job functions

# Account Management Do's and Don'ts

- **DON'T** share your user ID and password with anyone else.
- **DON'T** write your password down or keep it in an area where it can be easily discovered.
- **DON'T** use the "**remember password**" feature.
- **DO** remember that user accounts are disabled after three (3) consecutive **invalid attempts.**
- **DO** register with **official work email**; not unofficial/free email accounts.
- **DO** follow the MSIX Password Policy – A password 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;*
  - *Not be one of user's previous six (6) passwords.*

# POP-Quiz #1: Password Rules Q&A

Beth is trying to log into MSIX but isn't sure of her password.

Q1: Should she try to guess the password to sign-in?

Q2: She is embarrassed to ask her user administrator to reset the password. Should she ask her teammate to share their password with her?

Q3: Who should Beth contact to have her password reset?

Q4: Should Beth be embarrassed?

# POP-Quiz #1: Password Rules Q&A

Beth is trying to log into MSIX but isn't sure of her password.

Q1: Should she try to guess the password to sign-in?

A1: Yes, she can make up to 3 attempts before her account gets locked.

Q2: She is embarrassed to ask her user administrator to reset the password. Should she ask her teammate to share their password with her?

A2: No, never log in with another person's password.

Q3: Who should Beth contact to have her password reset?

A3: Beth should contact her User Administrator. They can be contacted through the MSIX login page. The MSIX Help Desk cannot assist with password resets.

Q4: Should Beth be embarrassed?

A3: No. Resetting passwords frequently is a very good practice.

# Email Best Practices

- Do not open unexpected attachments
- Do not click on suspicious links within emails
- Install and update anti-virus software on all devices
- 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
- Don’t give your email address to sites you don’t trust
- Suspicious emails must be reported as an incident to your IT office and to MSIX Help Desk

# POP-Quiz #2: Email Phishing

David receives the email message below. Is this legitimate?

From: IT Support Help Desk mvivisel@xcvb.com

To: David.Smith@ed.state.gov

Subject: Password Security Check

Attachment: passwordhack.exe

URGENT! REQUIRED!

You're IT support desk is providing a service to all users so you have good passwrods. click on attachment to check your passsword.

OR you can click on this link: http://passwordcollector.hax.com

Your account will be locked if you do not act now.

Password Team

# POP-Quiz #2: Email Phishing

David receives the email message below. Is this legitimate?

From: IT Support Help Desk mvivisel@xcvb.com

To: David.Smith@ed.state.gov

Subject: Password Security Check

Attachment: passwordhack.exe

URGENT! REQUIRED!

You're IT support desk is providing a service to all users so you have good passwrods. click on attachment to check your passsword.

OR you can click on this link: http://passwordcollector.hax.com

Your account will be locked if you do not act now.

Password Team

**Answer 1: Address doesn't match name**

**Answer 2: Suspicious attachment**

**Answer 3: False sense of urgency**

**Answer 4: Poor grammar and misspellings**

**Answer 5: Suspicious hyperlink**

**Answer 6: Threat of account lock-out encourages action**

# MSIX Privacy Protections

- Lock your computer when leaving computer unattended
- Media (including reports) containing MSIX information should be stored in locked container during non-business hours
- Do not leave paper media with MSIX information in public areas
- Store digital information in an encrypted format where technically possible
- Media containing MSIX information should be properly cleansed or destroyed
- If the access which you have been granted within MSIX is more than required to fulfill your job duties, it should be reported to your MSIX User Administrator
- Do not disclose MSIX information to individuals without a “need-to-know” of the information in the course of their business

# POP-Quiz #3: TRUE or FALSE - Privacy and PII

1. Comment fields in MSIX can be used to share information that we collect through MDEs, like address or phone number.

2. MSIX IDs can be shared through email since only MSIX users can get more personal information on that student.

3. Comment fields are inside MSIX so it's safe to write-in SSN, medical conditions and disciplinary records.

4. Screenshots from MSIX can be emailed to MSIX Help Desk since they already have access to the data.

# POP-Quiz #3: TRUE or FALSE - Privacy and PII

1. Comment fields in MSIX can be used to share information that we collect through MDEs, like address or phone number.
   - **TRUE**: MDE lists are approved list of data collected within MSIX.
2. MSIX IDs can be shared through email since only MSIX users can get more personal information on that student.
   - **TRUE**: MSIX IDs are only accessible by authorized MSIX users.
3. Comment fields are inside MSIX so it's safe to write-in SSN, medical conditions and disciplinary records.
   - **FALSE**: Only MDE lists are approved. If it's not an approved data element, MSIX is not authorized to collect the data anywhere.
4. Screenshots from MSIX can be emailed to MSIX Help Desk since they already have access to data.
   - **FALSE:** Emails can be intercepted by hackers.

# *Certificate of Completion*

## 2018 MSIX Security and Privacy Awareness Training (0.5 hour)

Completed on

_____ (date)

*I certify attendance and completion for this training.*

_____

Attendee Name Printed

_____

Attendee Signature

*I have verified completion of the training by the attendee.*

_____

Supervisor Name Printed

_____

Supervisor Signature

***Certificate is valid only when completed by both the attendee and their supervisor.***

# Part 2: User Administrator Role-Based Training

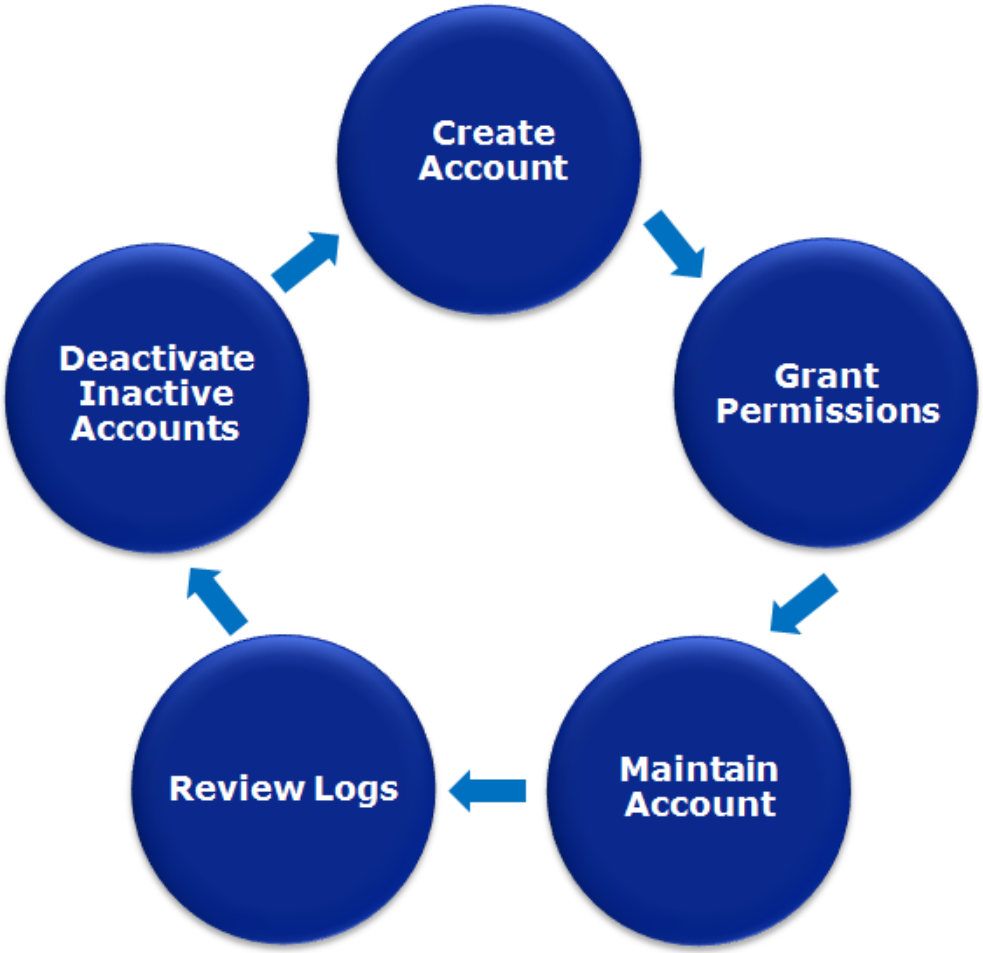
Non-User Administrators may drop off at this time.

# Part 2: User Administrator Role-Based Training

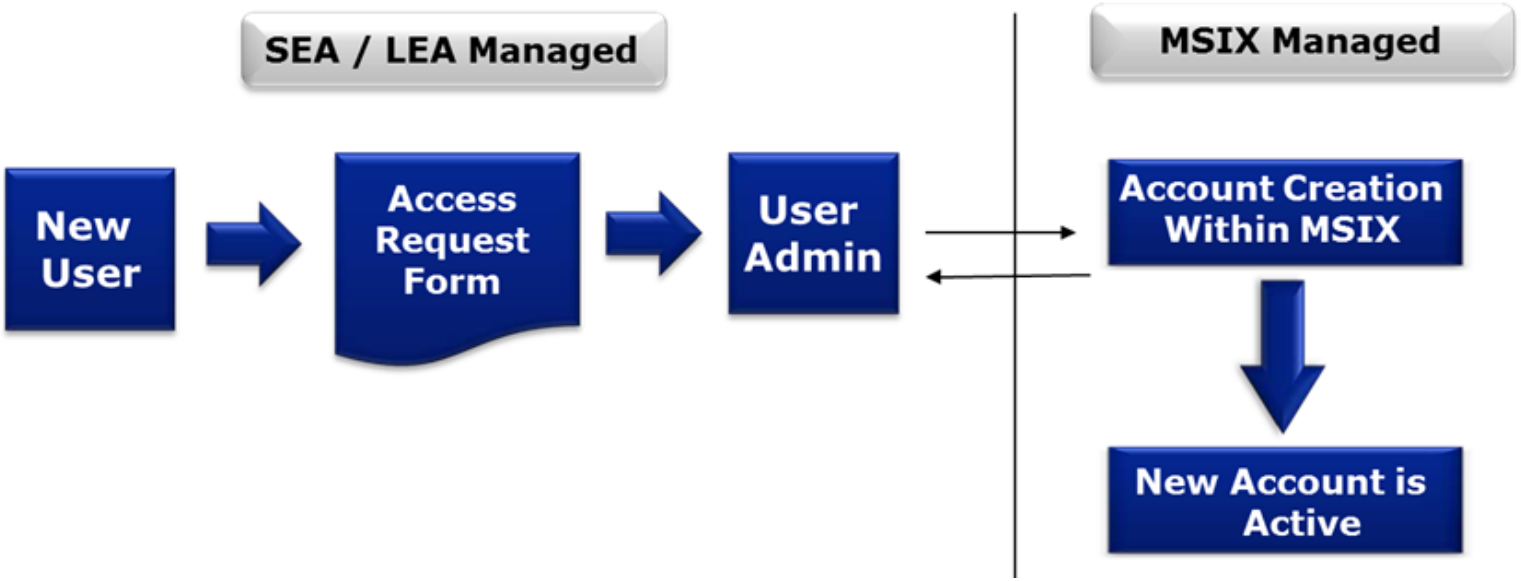
## Objectives:

- MSIX User Administrators will:
  - Understand each stage of the Account Management Cycle
  - Identify their role in the Account Management Process
  - Understand the difference between Privileged vs. Non-Privileged User Roles
  - Understand important principles of User Administration
  - Identify MSIX Report(s) available for periodic Account Reviews

# Account Management Cycle



# Initial Account Management Process




1. Account creation, modification and disablement are all handled by State or Regional User Administrator(s).
2. All request forms are maintained by the State.
3. Password resets are handled by State or Regional User Administrator(s).

# Privileged vs. Non-Privileged Accounts

- **Privileged User Roles** – able to perform user account management functions including creating, modifying and disabling or deactivating
  - State User Administrators
  - Regional User Administrators

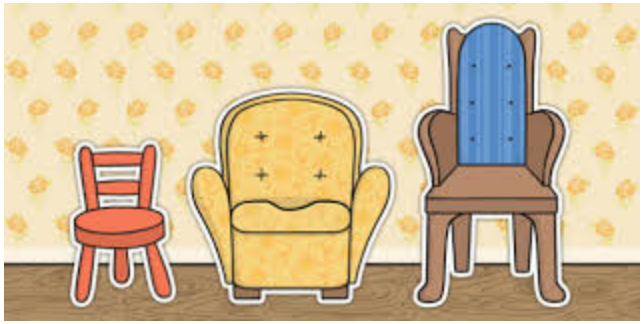
- **State Batch Submitters** – can upload files to MSIX

- **Non-privileged User Roles** – unable to perform user account management functions or upload files
  - MSIX Primary
  - MSIX Secondary
  - State Data Administrator
  - Regional Data Administrator
  - District Data Administrator
  - State Region Administrator

# User Administration Principles

- **Separation of Duties**
  - Having more than one person complete a task
- **Principle of Least Privilege**
  - Granting roles to perform only assigned job functions
  - Access “Need to know” information only
- **Examples**
  - Verifying authority and final approving authority should not be same person
  - A user should not have both MSIX primary and MSIX secondary role
  - A user should not be both a User Administrator and Data Administrator

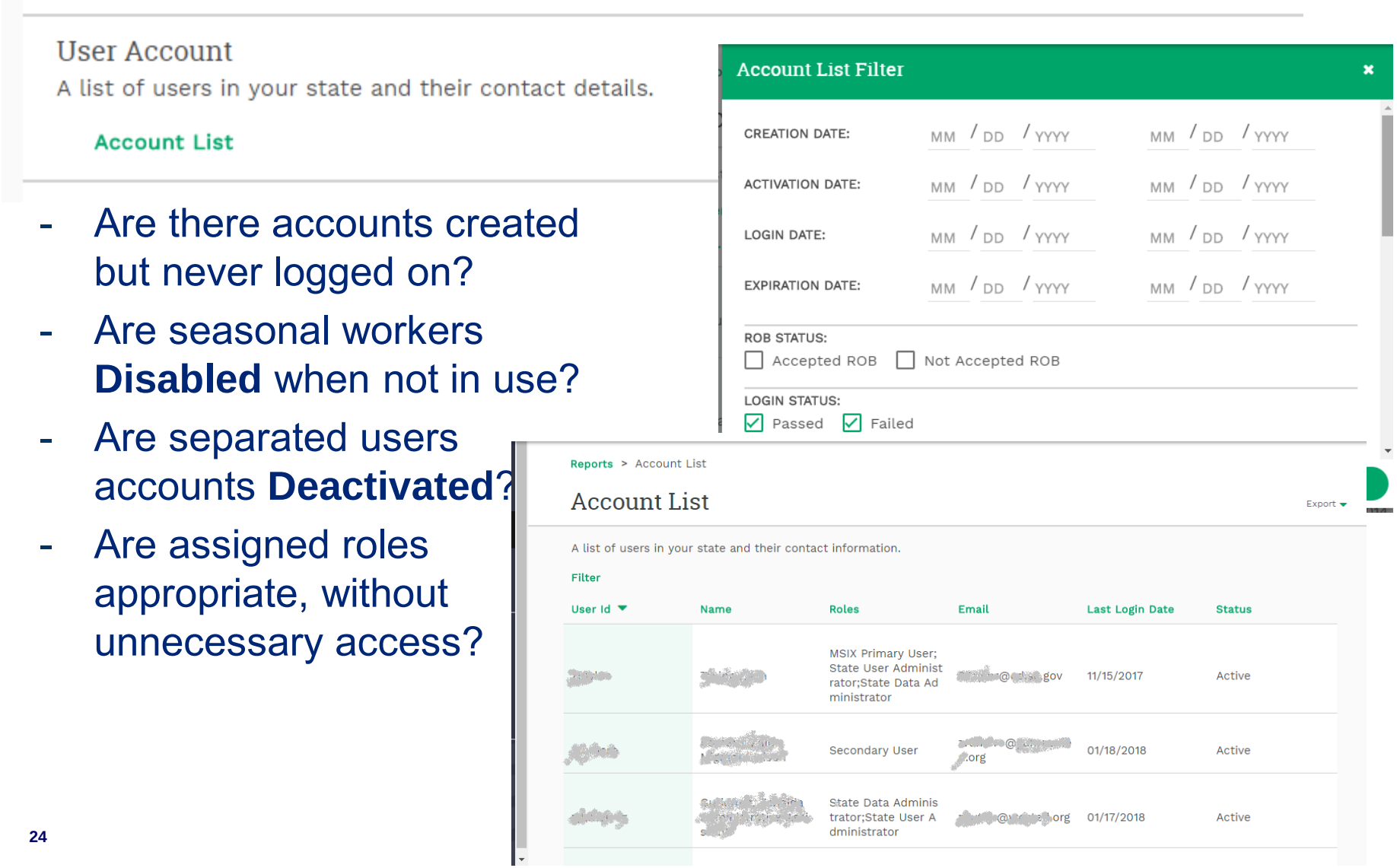
**Remember Goldilocks?**



# Account Reviews

- **Account Disablement** – account may be re-enabled
  - Seasonal program employees
  - Employee taking leave of absence
- **Account Deactivation** – permanent action in MSIX
  - Employee who has left job
  - Ensure that email address is changed upon deactivation
- **All accounts** should be **reviewed** at a minimum annually
  - Is user still employed in your State?
  - Is user still in same position?
  - Do assigned roles still make sense?

# User Administration Using Reports




- Are there accounts created but never logged on?
- Are seasonal workers **Disabled** when not in use?
- Are separated users accounts **Deactivated**?
- Are assigned roles appropriate, without unnecessary access?

# POP-Quiz: TRUE or FALSE – User Administration

1. MSIX User Administrators are privileged users because they can change other users' passwords, permissions and profile.

2. MSIX user accounts need periodic review.

3. MSIX User Administrators should encourage frequent password resets.

# POP-Quiz: TRUE or FALSE – User Administration

1. MSIX User Administrators are privileged users because they can change other users' passwords, permissions and profile.
   - **TRUE**: User Administrators must take extra care when changing user accounts at all times.
2. MSIX user accounts need periodic review.
   - **TRUE**: User accounts should be reviewed according to your State's MEP program cycles. MSIX Support team doesn't receive notice of changes in users' employment status.
3. MSIX User Administrators should encourage frequent password resets.
   - **TRUE:** Users are often embarrassed to request password resets when they are locked out. Users should be praised for frequent password changes, not shamed or blamed for forgetting it.

# *Certificate of Completion*

## 2018 MSIX User Administrator Role-Based Training (0.5 hour)

Completed on

_____ (date)

*I certify attendance and completion for this training.*

*I have verified completion of the training by the attendee.*

_____ Attendee Name Printed

_____ Supervisor Name Printed

_____ Attendee Signature

_____ Supervisor Signature

***Certificate is valid only when completed by both the attendee and their supervisor.***

# Wrap-Up