

# MSIX Cybersecurity and Accounts Management Webinar

---

**Maria Hishikawa / Sarah Storms**

February 6, 2019

# Agenda

---

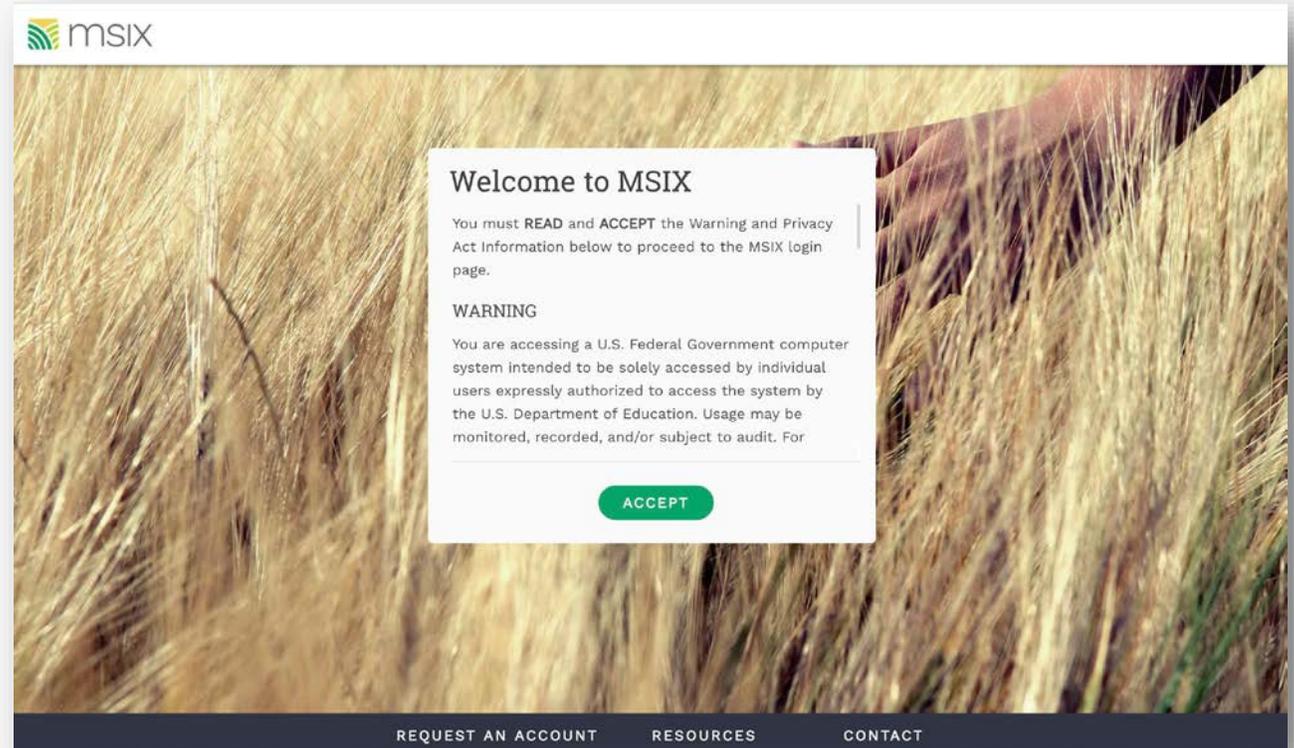
1. Introductions
2. MSIX Enhancements
3. Cybersecurity and Privacy Awareness Training (All)
4. User Administrator Training (User Administrators, MEP Directors)

A person's hands are shown typing on a laptop keyboard. The scene is set in an office with a desk, a smartphone, and some papers. The background is slightly blurred, showing other people working. The text "MSIX Enhancements" is overlaid in a bold, dark green font.

# MSIX Enhancements

# Recent Enhancements

- User must accept the Warning and Privacy Act Information **before** logging into MSIX
- User must acknowledge the Rules of Behavior **annually**



A person's hands are shown typing on a laptop keyboard. The scene is set in an office environment with a desk, a smartphone, and some papers. The image is overlaid with a semi-transparent grey filter.

# **Cybersecurity and Privacy Awareness Training**

# MSIX Help Desk Communications

---

- Do not send or provide **password information** to the MSIX Help Desk.
- **MSIX screenshots** and **PII** are rarely needed by the MSIX Help Desk to assist with an MSIX issue. If they are needed, the MSIX Help Desk will assist with proper ways to transmit minimal information needed to provide support.
- **Completed user account application forms** should not be sent to the MSIX Help Desk. Follow your State's procedures for retaining the applications.

# Password Security Reminders

---

- Never share your **user ID** and/or **password** with anyone else. You are responsible for all actions taken with your user credentials.
- The MSIX Help Desk will **never** request your password.
- **Do not write** your password down or keep it in an area where it can be easily discovered.
- Try using a **Password Phrase**

MSIX is great = M\$IXisGR8

# Media Protection

---

- **Media (paper, hard-drive, USB drive, memory card, etc.)** containing MSIX information should be **removed** from open spaces, such as desks and meeting rooms, and **stored** in a locked office or container during non-business hours.
- Do not leave **paper print-outs** with MSIX information in **public areas** such as printers, copiers, fax machines, conference rooms, coffee shops, etc.
- Be cognizant of “**shoulder surfers**” when reviewing MSIX paper media in public.
- Store **digital information** in an **encrypted format** where technically possible.
- Follow State procedures for **cleansing** or **destroying** media containing MSIX information.

# *Certificate of Completion*

---

## 2019 Basic Cybersecurity and Privacy Awareness 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.*

# BREAK TIME

## MSIX Help Desk

Email: [msixsupport@Deloitte.com](mailto:msixsupport@Deloitte.com)

Telephone: 1-866-878-9525

9:30 AM - 6:30 PM Eastern Time

Monday through Friday, except Federal Holidays

This concludes Basic Cybersecurity and Privacy Awareness for all MSIX Users.

Thank you for your attention and participation.

The next session is for User Administrators and State MEP Directors.

We will resume on the same conference line after a short break.

A person's hands are shown typing on a laptop keyboard. The scene is dimly lit, with a large monitor visible in the background. In the foreground, there are some papers and a smartphone. The overall atmosphere is professional and focused on learning.

# **User Administrator Training**

# Terminology Review

---

## **Active**

→ An account with successful logins within the last 90 days

## **Locked**

→ An account with 3 repeated login attempts using incorrect passwords

## **Expired**

→ An account without a password change in over 90 days

# Terminology Review

---

## **Disabled**

→ Action has been taken by a user administrator;  
temporary state; the same account may be re-enabled

## **Deactivated**

→ Action has been taken by a user administrator;  
permanent state; a new account must be requested

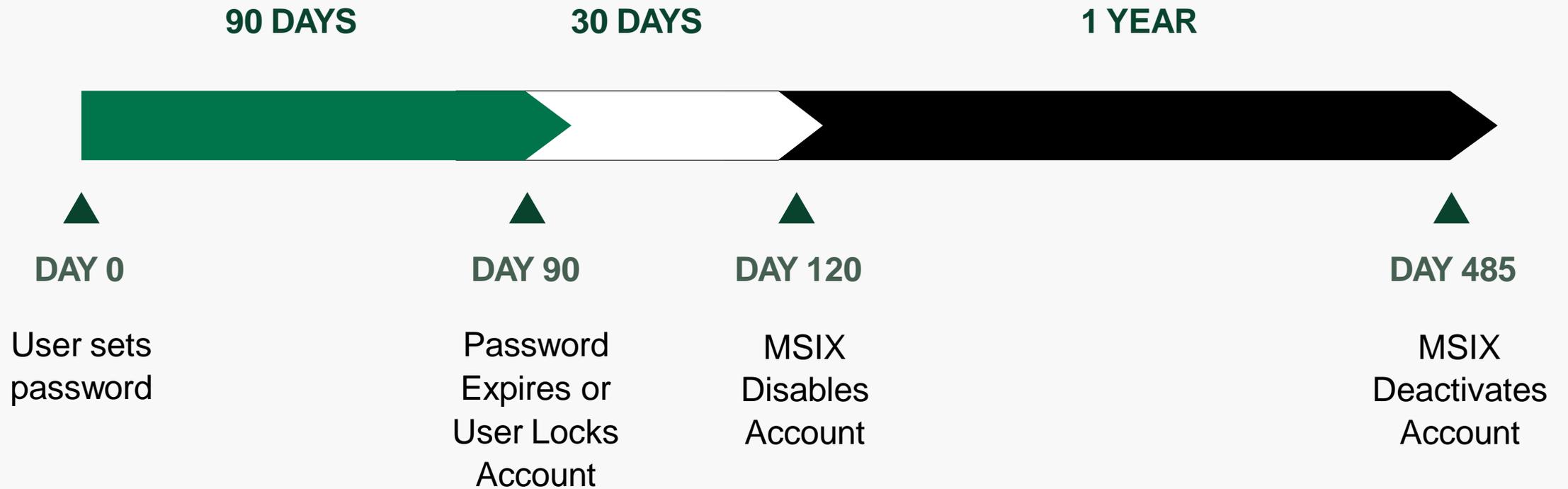
# Upcoming Changes

---

- Temporary passwords issued by MSIX will expire within **14 days** of issuance
- MSIX Team will enable **automated disabling and deactivating** of accounts
- User account reports will differentiate between **active**, **locked**, and **expired** accounts

# Proposed Automation Timeline

---



# Real World Scenarios

---

**Scenario 1:** Pam is a full school year employee. Her MSIX account is enabled for the start of the new school year in August. Pam continues to use her MSIX account for Fall Semester but does not access MSIX in the Spring or Summer. When Max, the State User Admin performs his yearly account review in August, what is the status of Pam's account?

- A. Disabled
- B. Deactivated
- C. Active
- D. Locked



# Real World Scenarios

---

**Scenario 2:** Lisa is a summer only MSIX user and is expected to return next summer. Her user account was activated June 1 and used through August 1. User Admin performs yearly account review at the end of August, what is the current status of the account and what action should user admin take on that account?

A. Active; Deactivate

B. Disabled; Do Nothing

C. Disabled; Deactivate

D. Active; Disable



# Real World Scenarios

---

**Scenario 3:** Tim was active in the 2016 – 2017 school year. His last password reset was in June 2017. Tim left the program in July 2017. He returns to work in February 2019 and requests a new MSIX account. What state is Tim’s user account in and what should the user administrator do?

- A. Disabled; Re-enable account
- B. Active; Reset password
- C. Deactivated; Require Tim to complete new request form
- D. Deactivated; Immediately reactivate



# User Administrator Responsibilities

---

- **Deactivate** user accounts for employees who have resigned.
- **Disable** user accounts for employees who are going on a leave of absence or are seasonal employees.
- Perform **yearly** account reviews of all user accounts.
- Verify **need-to-know** before re-enabling disabled accounts.
- Require **new user account form** before creating a new account for a user who has a previously deactivated account.

# *Certificate of Completion*

---

## 2019 MSIX User Administrator Privileged User 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.*

# Questions



# Thank you.

## **Maria Hishikawa**

**Contact:** [Maria.Hishikawa@ed.gov](mailto:Maria.Hishikawa@ed.gov)

## **Sarah Storms**

**Contact:** [SStorms@Deloitte.com](mailto:SStorms@Deloitte.com)

## **MSIX Help Desk**

**Email:** [msixsupport@Deloitte.com](mailto:msixsupport@Deloitte.com)

**Telephone:** 1-866-878-9525

9:30 AM - 6:30 PM Eastern Time

Monday through Friday, except Federal Holidays