

Time	Saratoga 1	Saratoga 2	Saratoga 3	Alabama	Travers	Broadway 1	Broadway 2	Broadway 3	Broadway 4
7:30am-8:30am	BREAKFAST			 All-District Conference					
8:00am-9:00am	Opening Remarks								
9:00am-9:30am	Vendor Booth Visits								
9:30am-10:20am	SchoolTool: Online Registration			RIC Lead Session <i>*By invite only</i>	MOOV: A Paradigm Shift in Attendance & School Safety	Advanced Analytics: Future of AA	SchoolTool: Attendance Refactor	MTSS Edge: Documenting RTI Meetings	ClearTrack: Demo (101)
10:30am-11:20am	SchoolTool: Custom Exports			Advanced Analytics: RIC Staff: Regional Successes	Ed Vistas: Breaking Language Barriers: Delivering Student Reports to Every Family	SchoolTool: Parent Experience	SchoolTool: Data Integrations	MTSS Edge: Supporting Your Staff	ClearTrack: New Features
11:30am-12:30pm	LUNCH								
12:40pm-1:30pm	Rollout Session		MTSS Edge: New Features	SchoolTool: BOCES	Mindex: Ed-Fi <i>*By invite only</i>	SchoolTool: Quality of Life	Advanced Analytics: Organizing Your Data for Authoring	MTSS Edge: Demo (101)	ClearTrack: Word Letters 101
1:40pm-2:30pm	SchoolTool: Security Tips & Tricks		SchoolTool: Standards-Based Grading	Advanced Analytics: Bringing Data into AA	AWS: AWS QuickSuite & Mindex AA: Secure, AI Powered Analytics for Education	Advanced Analytics: 101	SchoolTool: Leveraging SchoolTool for Summer Program Management	MTSS Edge: Class List Maintenance	ClearTrack: Spring/Summer Maintenance
2:40pm-3:30pm	SchoolTool: CCCR/NY Inspires			SchoolTool: Service Delivery Office Hours	ClassLink: Bridging System to Drive Impact: SchoolTool, ClassLink, & the power of APIs	Advanced Analytics: Gen BI & Author Session	Advanced Analytics: Newest Dashboards	MTSS Edge: Leveraging the Review Universal Scores Screen	ClearTrack: Data Warehouse Reporting





This document and the contents herein are Mindex Confidential Information and cannot be shared. We provide the presentation for informational purposes only, and the content herein does not create any commitments or assurances from Mindex. This document is not part of, nor does it modify, any agreement between Mindex and you.

Security Tips & Tricks

Security Tips and Tricks

Agenda

- Mindex → Recent Updates and Upcoming Work aligned to NIST CSF 2.0
 - Govern
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover
- District → How they handle SchoolTool security



Mindex – Recent Updates & Upcoming Work

Shared Responsibility Model aligned to NIST 2.0 CSF

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Build SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration

Nothing new to share in Identify or Respond

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Build SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration

Govern

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Build SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration

Govern

Mindex worked with the RIC One ROC to establish a central DPA; benefits include:

- **Unified Compliance:** Meets NYS Ed Law 2-d & NIST CSF.
- **Centralized Vetting:** Pre-approved by ROC TEC security reviews.
- **Easy Adoption:** Simple "Exhibit E" opt-in for districts.
- **Standardized Protection:** Consistent PII protocols region-wide.
- **Reduced Overhead:** Eliminates redundant district legal reviews.
- **Ongoing Partnership:** Continuous collaboration with RIC ONE.



Protect

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Provide SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration



Username

Password

LOG IN [Forgot Password](#)

OR

 Sign in with Google

 Sign in with Microsoft

 [Read the latest SchoolTool news](#) →

Security Rules

Password Minimum Length: 8

- ☒ Password Requires Upper Case Letters
- ☒ Password Requires Lower Case Letters
- ☒ Password Requires Numbers

Lock Accounts after 25 Failed Attempts in 5 Minutes

Protect

SchoolTool supports:

- Authentication & Authorization:
 - Local Logins; plus,
 - SSO via Okta, Classlink, Google, and Microsoft; and,
 - Groups via Okta, Classlink, and Entra
- MFA:
 - Directly in SchoolTool for Local Logins; and for,
 - SSO you should use 3rd party MFA on Identity Provider
- Local Logins:
 - Password expiration dates and length requirements
 - FYI - NIST recommends long over complex passwords (min 15 chars) since Aug/Sep 2024.



Protect

Over the past year we have:

- Phased out RDP access to servers
- Implemented CIS hardened instances
- Added ability to disable local logins
- Updated the forgot password workflow



Forgot Password

You'll need to enter your email address (associated with your account) to receive a temporary authorization code to reset your password.

Email *

SEND CODE

Authentication Code *

RESET PASSWORD

SchoolTool® Version 23.1-11
© 2025 Mindex • [Privacy Policy](#) • [Terms & Conditions](#)

Protect

Coming soon:

- Custom error messaging – eliminates the use of verbose errors, provides users with error ref. code.
- Session timeout updates – improves the user experience around extending sessions upon expiry and how we handle unextendible sessions (89067)
- Limit teacher access to student data for non-roster students (87005)
- Retirement of LDAP/s – reduces latency, avoids cert expiration issues, allows for IAM updates
- CloudFront CDN – Shifts request processing from our load balancers to the “edge” to further help abate DDoS attacks from flooding infrastructure

Custom Error Messaging – Design

Something went wrong...

Contact your support person with the following details:

1. Describe what you were doing when this error occurred
2. Copy the Error ID, Timestamp, and URL information below

Error ID: ST-2026-2-11-ABC123
Timestamp: 2026-02-11T11:52:05:00
URL: <https://schooltool.com/error>

Detect

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Provide SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration

Detect

Over the past year:

- Local network traffic – Be aware, we have seen several instances where user traffic has been blocked by web filtering and security applications on the district LAN (e.g., Lightspeed)

Coming soon:

- Permissions Dashboard
- Audit Log dashboard -- in Beta now



User Permissions

Table will show a green checkmark if the user has the given permission, otherwise the cell will be blank

	admin10@mdx.com	admin2@mdx.com	admin7@mdx.com	admin8@mdx.com	aprinz@comsewoga...	blu@mindex.com	ccarter@mindex.com
Rows	Has Feature	Has Feature	Has Feature	Has Feature	Has Feature	Has Feature	Has Feature
Attendance/Attendance Policy					✓	✓	✓
Attendance/Attendance Report					✓	✓	✓
Attendance/Attendance/Edit Minutes/Allow Batch Edit Minutes						✓	✓
Attendance/Attendance/Edit Minutes/Allow Exceeding of Minutes						✓	✓
Attendance/Attendance/Edit Minutes/Edit Minutes						✓	✓
Attendance/Attendance/Enter					✓	✓	✓
Attendance/Attendance/View Minutes					✓	✓	✓
Attendance/Audit Reports					✓	✓	✓
Attendance/Batch Make Present					✓	✓	✓
Attendance/Daily Attendance Mouse-overs					✓	✓	✓
Attendance/Daily Roster Report					✓	✓	✓
Attendance/Enter					✓	✓	✓
Attendance/Hide Remote Attendance Columns					✓	✓	✓
Attendance/Home District Report					✓	✓	✓

Controls

Action Person
Haley, Ryleigh

Action Person ID
All

Target Person
All

Target Person ID
All

Module
All

Submodule
All

Changed Information
All

Start Date
2025/12/01
YYYY/MM/DD

End Date
2025/12/31
YYYY/MM/DD

Date	Audit Log	Action Person	Action Person Name	Target Person	Target Person Name	Module	Sub Module	User	Text
Dec 2, 2025	10709	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 4, 2025	10712	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 8, 2025	10713	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 10, 2025	10716	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 15, 2025	10718	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 15, 2025	10719	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 15, 2025	10720	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 15, 2025	10721	146574	Haley, Ryleigh	null	null	General	Login	null	Logged in as lauren@mindex.com (Local Acc
Dec 15, 2025	10722	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Bulb
Dec 15, 2025	10723	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Cou
Dec 15, 2025	10724	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Gra
Dec 15, 2025	10725	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Spe
Dec 15, 2025	10726	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Sch
Dec 15, 2025	10727	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Atte
Dec 15, 2025	10728	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Rep
Dec 15, 2025	10729	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Year Rollover	null	Rollover from 2024-2025 to 2025-2026; Man
Dec 15, 2025	10730	146574	Haley, Ryleigh	146574	Haley, Ryleigh	Home	Preferences	null	Mod: Default School Year from 'All' to '2025-2
Dec 15, 2025	10731	146574	Haley, Ryleigh	146574	Haley, Ryleigh	Home	Preferences	null	Mod: Default School Year from '2025-2026' to
Dec 15, 2025	10732	146574	Haley, Ryleigh	44136	Rivera, Colten	Census	Student > Enrollment	null	Mod: Official Enrollment for 7/1/2024 - 6/3/
Dec 15, 2025	10733	146574	Haley, Ryleigh	44136	Rivera, Colten	Census	Student > Enrollment	null	Mod: Official Enrollment for 7/1/2024 - 6/3/
Dec 15, 2025	10734	146574	Haley, Ryleigh	44136	Rivera, Colten	Census	Student > Enrollment	null	Add: Official Enrollment: Enroll Building or Gr
Dec 15, 2025	10735	146574	Haley, Ryleigh	null	null	Maintenance	School Year > Cycle Day Scheme Assignment	null	Mod: Cycle Day Scheme from 'None' to 'All' h

Recover

NIST 2.0 Function	Mindex (Cloud & Application)	RIC & District (Data & Access)
Govern	• Manage AWS supply chain risk • Maintain corporate 2-d compliance	• Appoint Data Protection Officer (DPO) • Manage DPA & Parents' Bill of Rights
Identify	• Map application PII data flows • Scan code for vulnerabilities	• Maintain Data Privacy Inventory (DPIT) • Inventory local devices & "Shadow IT"
Protect	• Enforce AES-256 / TLS 1.2+ encryption • Provide SSO, MFA, & Role-Based Access Control	• Provision user accounts & local MFA • Conduct annual Ed Law 2-d training
Detect	• Monitor AWS infrastructure anomalies • Alert on application-level threats	• Monitor local network traffic • Audit staff data access & behavior logs
Respond	• Execute Mindex Incident Response Plan • Provide forensic logs & breach details	• Execute local Incident Response Plan • Notify NYSED Privacy Office & parents
Recover	• Maintain geo-redundant AWS backups • Restore core application & databases	• Activate local Business Continuity Plan • Validate data integrity post-restoration

Mindex: Business Continuity & Disaster Recovery Summary

Document Version: 1.0 Last Updated: November 5, 2025

1. Our Commitment to Your Business Continuity

At Mindex, we take the resilience and availability of your services seriously. We have invested in a Business Continuity and Disaster Recovery (BCDR) program designed to protect your operations from significant disruptions.

This document provides a summary of our preparedness, our service commitments, and the communication plan you can expect from us during a service-disrupting event.

2. How We Ensure Service Resilience

Our BCDR strategy is built on industry best practices to ensure our critical systems and your data are protected and recoverable.

- **Redundant Infrastructure:** Our primary production environment is built with high-availability and redundancy to prevent small-scale failures from impacting service.
- **Secure Data Backups:** Your data is backed up regularly to secure, geographically separate locations. All backup data is encrypted in transit and at rest.
- **Regular Testing:** We conduct regular tests of our DR plan, including data restoration and system failover, to ensure our procedures are effective and teams are prepared.
- **Access & Security Controls:** We maintain strict security protocols to protect our infrastructure from unauthorized access, data breaches, and other cyber threats.

3. Our Service Level Objectives (SLOs)

We measure our recovery capabilities using two key industry metrics. These are our internal targets that guide our DR plan.

- **Recovery Time Objective (RTO):** This is our target for the **maximum time** it should take to restore service following a declared disaster. Our target is to **restore critical services within 4 hours** of declaring a disaster-level event."
- **Recovery Point Objective (RPO):** This is our target for the **maximum acceptable amount of data loss** in a worst-case scenario. This is determined by our backup frequency. In the event of a total disaster, our plan is designed to ensure **no more than 15 minutes of data is lost**.

What does this mean? We aim to have the service back online within 4 hours and that any data entered in the 15 minutes leading up to the failure is the most that is impacted.

Recover

Mindex shared a Customer-facing DR Plan post AWS outage:

- Shared upon request with contract holders as it contains proprietary information:
 - RICs
 - Direct Customers
- Outlines our:
 - Service-Level Objectives
 - How we Communicate
 - Your Responsibility in disaster scenarios
- For Common Disaster Scenarios we provide:
 - Mitigation Strategies that we have taken
 - What to expect (re: SchoolTool availability) if it occurs

District Speaker – Groups, Users & Privileges Deep Dive

Student Management System Groups, Users and Privileges: A Deep Dive

(plus bonus tips!)

Scan me!
(if you trust me)

Kieran O'Connor, ESM Schools

Executive Director of Planning, Development & Technology
Data Privacy Officer

Presentation: esmschools.org/oconnor



Kieran O'Connor

- East Syracuse Minoa Schools
- Exec Dir: Planning, Dev., & Technology
- Data Privacy Officer
- PreK-12--3,500 students, CNY
- koconnor@esmschools.org
- 315-434-3008
- Schools we share in common?



Goals of Presentation

- Provide examples of how you can think about SMS data security
- Provide strategies you can bring to your District
- Collaborate on real life examples
- Address audience questions/scenarios

Overview

We will discuss/think about:

- Setting up groups in your SMS, and assigning privileges to those groups
- Adding/managing people in user groups, based on their job needs
- Performing self audits

Question:

- Have you reviewed your SMS groups and privileges in the
 - Last year
 - Five years
 - Ever?
- How about a review of **users** assigned to those groups?

- User group review

- Do you have the **right** groups?
- Do you need to consolidate or create new groups?
- **THEN** review privileges in your groups.

- Your list of groups should be simple enough that whoever assigns SMS access knows what to do
- Teachers get the “Teacher Group,” etc
- Create whatever groups you need
- You may need to add/delete them over time
- If in doubt, UNDER privilege your groups

- ☐ SMS_Attendance
- ☐ SMS_BasicAccess
- ☐ SMS_CensusSearch

- ☐ SMS_Teachers
- ☐ SMS_TeachingAssistant
- ☐ SMS_Transportation

Here are some of the permissions one of our groups has

Student/Alert/Medical Alert/Icon	1		*
Student/Alert/Medical Alert/Mouseover Information	1		*
Student/Contacts/Enter	1		*
Student/Contacts/Show Call Order	1		*
Student/Contacts/Show Custody Alert Icon	1		*
Student/Contacts/Show Parent Portal Access Icon	1		*
Student/Contacts/Show Pickup Icon	1		*
Student/Contacts/Show Primary Contact Icon	1		*
Student/Contacts/Show Receives Mail Icon	1		*
Student/Contacts/Show Student Display Name for Contact	0		
Student/Discipline/Enter	1		*
Student/Discipline/Print Incident	0		

- ***Demo of SMS groups report
- Now that you have reviewed your groups and privileges, the next step is to review WHO is in each group
- Take the time to go over the lists carefully
- If in doubt, **remove** the person from the group. DO NOT HESITATE!

- Better to remove user access and let them ask for it back. No one ever says “I have too much access”
- Create an account matrix, add BOCES/other partners too (next slide)
- ***Demo of SMS user report

FAKE
DATA

Position type	Google	Schooltool	Network Logon	nVision	staff intranet
District-wide Administrator	Y	Y	Y	Y	Y
Building Administrator	Y	Y	Y	N	Y
Non-Instructional Supervisor	Y	Y	Y	N	Y
Network Admin	Y	Y	Y	N	Y
Lan Tech	Y	Y	Y	N	Y
Nurse	Y	Y	Y	N	Y
Head Custodian	Y	N	Y	N	Y
Custodian / Custodial Worker	Y	N	Y	N	Y
Food Service Manager	Y	Y	Y	N	Y
Food Service Worker	Y	Y	Y	N	Y
Mechanic	Y	N	N	N	N
Delivery Person	Y	Y	Y	Y	Y
Transportation admins	Y	Y	Y	Y	Y
Bus Driver	Y	N	N	Y	Y
Secretary or Typist	Y	Y	Y	Y	Y
Teacher / school psychologist/OT/PT / Speech Pathologist	Y	Y	Y	Y	Y
Teaching Assistant	Y	Y	Y	Y	Y
Teaching Assistant (Long Term)	Y	Y	Y	Y	Y
Teacher Aide	Y	Y	Y	Y	Y
Student Teacher	Y	Y	Y	Y	Y
Daily (Per-Diem) Sub	Y	Y	Y	Y	Y
Long Term Sub	Y	Y	Y	Y	Y
Regular Sub	Y	Y	Y	Y	Y
Sub Counselor	Y	Y	Y	Y	Y
Sub Nurse (regular)	Y	Y	Y	Y	Y
Sub nurse (long term)	Y	Y	Y	Y	Y
Long Term Sub Counselor	Y	Y	Y	Y	Y

FAKE
DATA

- During user review, you will find:
 - Staff have changed roles, and need to shift to other groups, or lose access completely
 - Some need additional privileges. If so, give them an additional group(s) (“stacking”), **don’t** add the privilege to the current group

Things to think about

- Staff/parent accounts should be separate for data security! **Don't** use school email for parent access--why?
- You may need help with account management from HR, or other office(s)

- It's not personal! It's "need to know"
- It's also about risk reduction
- Exceptions need a formal request from a supervisor, and approval from the SMS admin
- Document the request and approval!
No exceptions. We get audited!

- When staff leave, remove their SMS group from their SMS user account
 - We use retirees a lot, but their roles are different. HR guy is now on special projects.
- Watch for account re-use: Student→ Parent→ Staff. You are editing history

- Superusers--should be limited
- BOCES & Mindex staff: create a Superuser lite, move people as needed
- Does BOCES/Mindex have MFA?

- OK, you've done all the work, you're done, right? Nope, now do audits of
 - Groups--adjust them if needed, including privileges (every other year)
 - Users--confirm users in groups (annual)
 - July 1 disable **all** BOCES/Partner accounts/SMS provider/etc

Final Thoughts

- It's painful
- It will take hours to do it
- People won't like you
- But chip away at it!
- “Security always wins” (Kieran-ism)

Bonus Tips

Bonus 1: Registration Communications

- How are you sending and receiving records?
 - **Externally**--encrypted email, secure portal, fax, US Mail, other?
 - **Internally**-- (next slides)

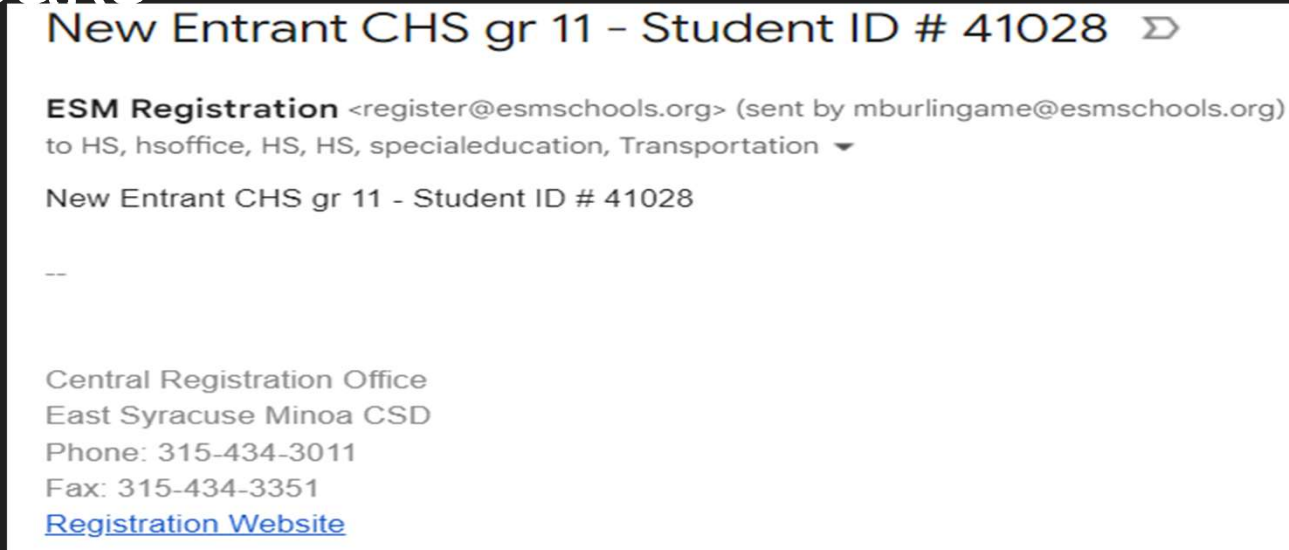
Bonus 2: Registration Docs

- Sort and categorize your registration docs. Add in buckets
- Info is “need to know,” not one packet



Bonus 3: Registration Communications

- Internal: don't send registration files or info, just send the ID and refer them to your SMS
- Prevents data leaks



Bonus 4: Registration Email/VMail

- Setup Group email addresses, NOT forwarders
 - register@esmschools.org
 - FEOffice@esmschools.org
- Route voicemails to the group email addresses
- Provides for coverage, keeps data in one account
- Quick demo

Bonus 5: Registration Office

- Our new parents are mid 20-30's: not using voicemail or answering calls
- Cell phone for the office, to make it easier to contact parents by texting
- Used in Registration and HR

Bonus 6: Superuser

- Don't be a superuser for your everyday account
- Create a separate account to use as superuser when you need it
- Downgrade BOCES/Mindex, easy to add as needed
- It's about RISK, not trust

Bonus 7: Google/O365 Logins

- Default is to force login to once a week, set it to 20 hours in “session control”
- Turn off “allow user to trust the device” for MFA
- Why do this? It’s your login for SMS-- staff are logged in at home....so

Special Thanks

- Terri Clark, CNYRIC. Schooltool Consultant onsite with us
- Amanda Hardin, CNYRIC. Sr. Database Designer. (Created the reports!)
- CNYRIC for putting up with me



Remember what Mr.
T says: “I pity the fool
who doesn’t use
SchoolTool!”

- Questions?
- Scenarios?
- Discussion topics?

Thanks!

Kieran O'Connor

koconnor@esmschools.org

315-434-3008

Scan for this
presentation, or

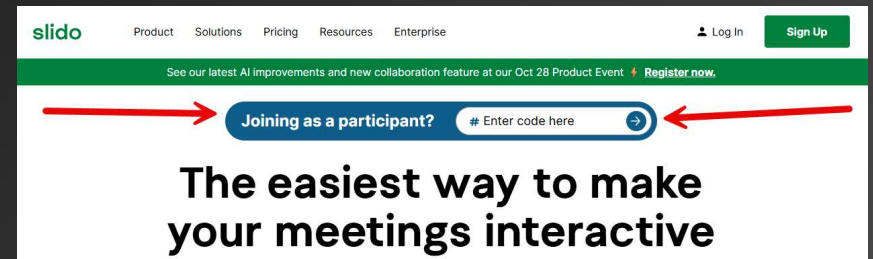
esmschools.org/oconnor



Interactive Survey – Please Participate!



Join at slido.com



Enter Code:
112 2830





ST: Security Tips & Tricks

① The Slido app must be installed on every computer you're presenting from

slido

Resources

[IT Governance, NY Comptroller](#)

[Data Classification](#) template



MINDEX

mindex.com