

Robbins Schwartz

**SOPPA Amendments
2021: Requirements for Written
Agreements and Strategies for Risk
Mitigation**

March 16th, 2021

Robbins Schwartz

LEARNING
TECHNOLOGY
CENTER of ILLINOIS



SECURE HALO
SECURING THE ENTERPRISE

 **GALLAGHER BASSETT**
GUIDE. GUARD. GO BEYOND.

SOPPA Amendments 2021: Requirements for Written Agreements and Strategies for Risk Mitigation MARCH 16, 2021

AGENDA

- Legislative background, definitions and scope of SOPPA, and overview of written agreement requirements (Matthew Gardner and Emily Bothfeld)
- Overview of NDPA and Illinois Exhibit and Illinois Student Privacy Alliance Resources (Chris Wherley and Tim McIlvain)
- Cyber liability coverage considerations and recommendations (Michael McHugh and Tyler Mackenzie)
- Security best practices (Will Durkee)
- Final recommendations and risk management strategies (Matthew Gardner and Emily Bothfeld)
- Q&A

Legislative Background



Robbins Schwartz

1

Legislative Background

- The *Student Online Personal Protection Act (105 ILCS 85/)* was first enacted in 2017.
- The Act placed various prohibitions on web operators that collect student information.

Robbins Schwartz

2

Legislative Background

- Public Act 101-0516, which amends the *Student Online Personal Protection Act*, was signed into law in August 2019.
- New requirements go into effect on July 1, 2021.

Robbins Schwartz

3

Definitions and Scope of SOPPA



Robbins Schwartz

4

Definitions

- “Operator” means the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. 105 ILCS 85/5.

Robbins Schwartz

5

Definitions



- “K-12 purposes” means purposes that are directed by or that customarily take place at the direction of a school, teacher, or school district; aid in the administration of school activities, including but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel or parents; or are otherwise for the use and benefit of the school. 105 ILCS 85/5.

Robbins Schwartz

6

Section 5: Definitions

- “Covered information” means personally identifiable information/material or information that is linked to personally identifiable information/material in any media or format that is not publicly available, and that is:
 - Created by or provided to an operator by a student or the student’s parent in the course of their use of the operator’s site for k-12 school purposes;
 - Created by or provided to an operator by an employee or agent of a school or school district for K-12 school purposes; or
 - Gathered by an operator through the operation of its site, service or application for K-12 school purposes and that personally identifies a student

105 ILCS 85/5.

Robbins Schwartz

7

Section 5: Definitions

- “Breach” means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or school. 105 ILCS 85/5.

Robbins Schwartz

8

Overview of Written Agreement Requirements



Robbins Schwartz

9

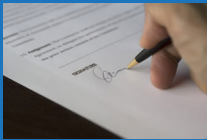
Written Agreement Requirements

- An operator who seeks to receive any covered information from a school district must enter into a written agreement with the school district before the covered information may be transferred. 105 ILCS 85/15(4).

Robbins Schwartz

10

Written Agreement Requirements



- Except in limited circumstances, a public school may not share, transfer, disclose, or provide access to a student's covered information to an entity or individual, other than the student's parent, school personnel, appointed or elected school board members, or the State Board, without a written agreement. 105 ILCS 85/26.

Robbins Schwartz

11

Written Agreement Components

- The written agreement must contain:
 - A listing of the categories or types of covered information to be provided to the operator;
 - A statement of the produce or service that the operator is providing to the district;

Robbins Schwartz

12

Written Agreement Components

- The written agreement must contain (continued):
 - A statement that the operator is acting as a school official under the Family Educational Rights and Privacy Act (“FERPA”);
 - A statement that the operator will implement and maintain reasonable security procedures and practices that meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, modification, or disclosure;

Robbins Schwartz

13

Written Agreement Components



- The written agreement must contain (continued):
 - A statement that the operator must delete or transfer to the district all covered information that is no longer needed for purposes of the agreement;
 - A statement that the written agreement will be published on the district’s website; and

Robbins Schwartz

14

Designation of Employees with Authority to Enter into Written Agreements

- Any agreement entered into in violation of SOPPA (i.e., by an individual other than those employees who are expressly authorized to enter into such agreements) is void and unenforceable as against public policy. 105 ILCS 85/27(b).

Robbins Schwartz

Learning Technology Center Student Online Privacy Protection Act (SOPPA)

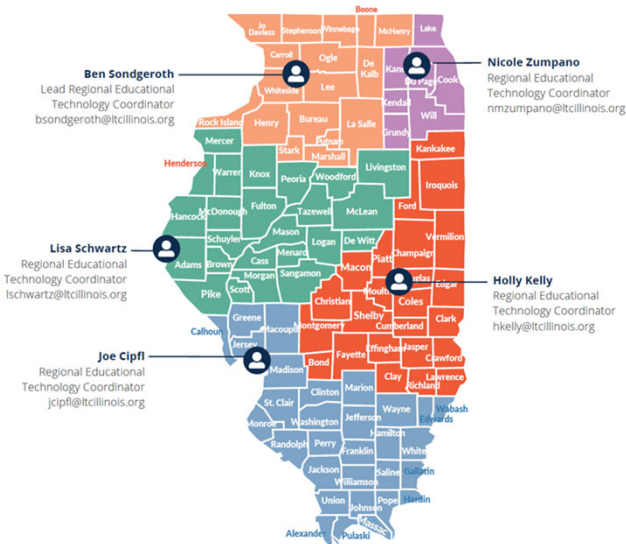


19

About the LTC

The **Learning Technology Center** is a statewide organization that provides technology services and professional learning.

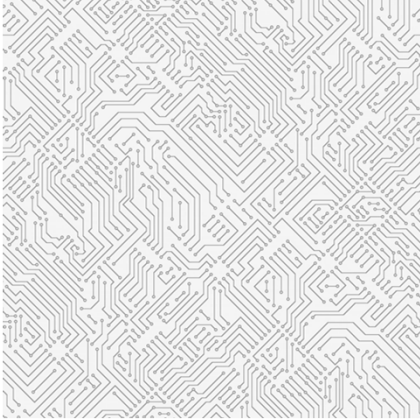
- Professional Learning & Events
- Digital Learning
- Technical Support
- Data Privacy & Cybersecurity
- Access & Equity
- Purchasing
- Communities of Practice



20

PROGRAM

National Data Privacy Agreement



The National Data Privacy Agreement (NDPA) was developed by 31 state alliances addressing data privacy needs. The LTC encourages districts to adopt the NDPA with the Illinois Exhibit to help streamline the educational application contracting process.

ltcillinois.org/services/ispa



21

PROGRAM

Illinois Student Privacy Alliance (ISPA) + NDPA



A free tool for managing privacy agreements in compliance with SOPPA. ISPA is a shared database that allows districts to:

- Manage and track agreements.
- “Piggyback” on agreements when another district in Illinois already signed an agreement.
- Post agreements, data elements, and subcontractors on your website.

ltcillinois.org/services/ispa



22

SOPPA Resources

- [Legislative Brief on SOPPA](#)
- [SOPPA Introduction Video](#)
- [Frequently Asked Questions](#)
- [Recommended Reasonable Security Practices](#)

ISPA Resources

- [Illinois Student Privacy Alliance \(ISPA\)](#)
- [Using ISPA to Comply with SOPPA \(Flowchart\)](#)
- [Managing Agreements with ISPA \(Flowchart\)](#)
- [Sample ISPA Communications](#)

ltpillinois.org/services/dataprivacy

ltpillinois.org/services/ispa





Cyber Liability Coverage


Michael McHugh, Area Senior Executive Vice President
 Tyler MacKenzie, Account Executive – Key Accounts
 March 16, 2021



Insurance | Risk Management | Consulting

©2021 ARTHUR J. GALLAGHER & CO.

25



Cyber Liability Insurance Coverage Overview

- Costs and expenses associated with a breach of district systems
 - Addresses Data compromised as a result of system breach (i.e. staff, students, etc.)
 - Addresses corruption or takeover of system by an intruder (i.e. Ransomware)
 - Addresses alleged Third Party damages from system breach
- Forensic Auditing
 - Determines what data may have been accessed
- Breach Counsel
 - Advises on statutory requirements based on data that was compromised

Breach Response Services Privacy Attorney, IT Forensics, Notification providers etc.	First Party Business Costs Extortion payments, Business Interruption, Data Restoration etc.
Third Party Costs Regulatory Fines, Third Party Damages etc.	Limit At least \$2,000,000 in the form of a standalone policy with a reputable insurer

©2021 ARTHUR J. GALLAGHER & CO.

26

Important Breach Response Features for School Districts

- Simple notification process – 1 single call to a 24/7 Breach Response Hotline
 - Handled by a reputable Cyber Security firm (ex. Phelps Dunbar)
 - No need for email/written notice and duplicated phone calls
- Access to a Breach Response firm
 - Should specialize in data privacy and security (ex. Baker Hostetler – handled Marriott and Capital One breaches)
- IT Forensics panel that includes well known firms
 - Ex. Kroll, Kivu, Mandiant, Coveware (for Ransom negotiations and payments)



27

©2021 ARTHUR J. GALLAGHER & CO.



Vendor Insurance Requirements

- Any vendor who will be storing, or accessing, sensitive district data should be required to maintain Cyber Liability coverage
 - A minimum limit of \$1,000,000 per claim
 - Limit should be increased depending on:
 - # of contracts / value of contract
 - Industry field
 - Significance, and amount, of Data being accessed
 - Aggregate Limit is Important
 - Ideally this is at least \$2,000,000 or more
 - Obtain a Certificate of Insurance Evidencing the contractually required coverage
- Depending on service being provided Technology Errors & Omissions may be needed as well (ex. IT Firm)
- Legal Counsel Review
 - Make certain this is done to see the district's best interests are addressed



28

©2021 ARTHUR J. GALLAGHER & CO.

Latest Ransomware Trends

Sharp increase in the average Ransoms demanded:

- 2017** – WannaCry & Not Petya – Ransom demanded was \$150 - 300
- 2018** – Baker Hostetler Report – Average Ransom paid was \$28,920
- 2019** – Baker Hostetler Report – Average Ransom paid was \$302,539
 - Rise in RYUK Ransomware – Average Ransom demand in Q4 of 2019 was \$779,856
- 2020** – Average RYUK Ransom demand in Q1 2020 was \$1,339,878
 - Average RYUK Ransom payment in Q3 2020 was **\$7,390,000**

29

COVID-19

Ransomware attacks increased 72% in the first half of 2020, amidst the COVID-19 global pandemic

How are hackers getting in?

- COVID-19 related Phishing emails – e.g. Principle's email purporting to contain a Covid-19 update or new set of guidelines
- Data sprawl post Covid-19 – e.g. Teachers/Staff emailing documents to their personal emails, to print on home computers
- Remote login vulnerabilities
- Lower security standards on home/public WiFi networks

30

Cyber Marketplace Conditions

- **Significant Ransomware losses, alongside 'traditional' Cyber losses have had a substantial impact on the insurance market:**
 - ❖ Not only in terms of rating:
 - 2019 = 5% - 15% Rate Increases
 - 2020 = 15% - 80% Rate Increases (little or no claims)
 - ❖ But also in terms of appetite:
 - Major Carriers withdrawing completely from the market – AXA XL, MS Amlin
 - Major Carriers withdrawing from particular classes – Beazley withdrawing from Public Sector & Education
 - Some carriers looking to exclude, sublimit, or coinsure Ransomware
- **More scrutiny on underwriting:**
 - ❖ Additional questions on renewal applications
 - ❖ **Minimum standards = Offsite segregated backups, MFA for remote login for all admin staff with access to sensitive data**
- **Rapidly Evolving Marketplace as frequency and severity of Ransomware Attacks continues to increase**

31

©2021 ARTHUR J. GALLAGHER & CO.

31

Best steps to avoid falling victim to Ransomware

- **BACKUP, BACKUP, BACKUP**
 - Frequency – regularly (weekly minimum)
 - Quality – all critical files and data
 - Location – on and off-site, segmented from production systems
 - Test Backups – establish procedures to regularly test Backups
 - Build restoring from Backups into Incidence Response Planning
 - Off-site backup required for coverage
- Avoid being Phished
 - Implement Employee phishing training
 - Use strong passwords – prevent duplication
 - Deploy an email threat filter



32

©2021 ARTHUR J. GALLAGHER & CO.

32

Best steps to avoid falling victim to Ransomware Cont.

- Secure Remote Access – Especially in current environment
 - Implement Multifactor Authentication (MFA) for remote access to systems and emails
 - **This is becoming a mandatory requirement for Cyber insurers to provide coverage**
 - Only implement Remote Desktop Protocol (RDP) where necessary
- Ensure that you regularly apply all patches (updates)
 - Attackers exploit software vulnerabilities which can be remedied by patches
- Deploy the following security measures:
 - Firewalls – configured properly
 - Endpoint Monitoring



33

©2021 ARTHUR J. GALLAGHER & CO.

33

Common Software with MFA Add-Ons

- Microsoft Office 365
- Google G-suites
- Both offer Tutorials
 - ✓ Google: “Microsoft MFA” and/or “G-suite MFA”

Thank you!

Michael McHugh / Tyler MacKenzie
630.285.4373 / 630.694.5165
Michael_McHugh@ajg.com / Tyler_Mackenzie@ajg.com



Gallagher

Insurance | Risk Management | Consulting

©2021 ARTHUR J. GALLAGHER & CO.



34



SECURE HALO
SECURING THE ENTERPRISE



SOPAA Security Requirements

35

Section 15:



“An operator shall... Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.”

TSCI Confidential and Proprietary Information not to be distributed.

36

36

Section 15:

“An operator shall... Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.”



TSCI Confidential and Proprietary Information not to be distributed.

37

37

Section 15:

“An operator shall... Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized **access**, destruction, use, modification, or **disclosure**.”



TSCI Confidential and Proprietary Information not to be distributed.

38

38

Section 15:

“An operator shall... Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.”



TSCI Confidential and Proprietary Information not to be distributed.

39

39

Section 15:

“An operator shall... Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.”

TSCI Confidential and Proprietary Information not to be distributed.

40

40

Section 15:

“An operator shall... Implement and maintain **reasonable** security procedures and practices that otherwise meet or exceed **industry standards** designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.”

NIST Cybersecurity Framework
 NIST 800-53
 NIST 800-61
 NIST 800-37
 SANS
 COBIT
 CIS
 ISO 27000 series

41

CIS Controls™

V7.1

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- | | |
|--|--|
| 7 Email and Web Browser Protections | 12 Boundary Defense |
| 8 Malware Defenses | 13 Data Protection |
| 9 Limitation and Control of Network Ports, Protocols and Services | 14 Controlled Access Based on the Need to Know |
| 10 Data Recovery Capabilities | 15 Wireless Access Control |
| 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches | 16 Account Monitoring and Control |

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

42

CIS Critical Security Controls Implementation



Know Your Assets

- 1. Hardware Inventory
- 2. Software Inventory
- 13. Data Protection
- 16. Account Monitoring and Control

TSCI Confidential and Proprietary Information not to be distributed.

43

CIS Critical Security Controls Implementation



Harden Your Assets

Cloud Solutions:

- 7. Email and Web Browser Protections
- 8. Malware Defenses
- 18. Application Software Security (if applicable)

Network:

- 3. Continuous Vulnerability Management
- 9. Limitation and Control of Network Ports, Protocols, and Services
- 11. Secure Configuration of Network Devices such as Firewalls, Routers, and Switches
- 12. Boundary Defense
- 15. Wireless Access Control

TSCI Confidential and Proprietary Information not to be distributed.

44

CIS Critical Security Controls Implementation



Harden Your Assets

Devices

5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

People

4. Controlled Use of Administrative Privileges

14. Controlled Access Based on the Need to Know

17. Implement a Security Awareness and Training Program

TSCI Confidential and Proprietary Information not to be distributed.

45

CIS Critical Security Controls Implementation



Resiliency

10. Data Recovery Capabilities

6. Maintenance, Monitoring and Analysis of Audit Logs

19. Incident Response and Management

20. Penetration Tests and Red Team Exercises

TSCI Confidential and Proprietary Information not to be distributed.

46

Recommended Path Forward

Assess what is currently in place
and what needs to be
implemented/documentd

Plan implementation steps

Document all controls

Operationalize security tasks

For more information:

<https://www.cisecurity.org/controls/>



TSCI Confidential and Proprietary Information not to be distributed.

47

Final
Recommendations
and Risk Mitigation
Strategies



Robbins Schwartz

49

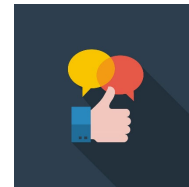
Final
Recommendations
and Risk Mitigation
Strategies

1. Designate at least one employee to oversee your district's compliance with SOPPA's requirements.
 - Could be Director of Technology, Records Custodian, or someone else.
 - Depending on the size of your school district, consider designating more than one employee to oversee compliance.

Robbins Schwartz

50

Final
Recommendations
and Risk Mitigation
Strategies



2. In conjunction with designated employee(s), conduct an inventory of all operators currently receiving covered information.
 - May require district-wide inquiry to all teachers and other staff members who work with students.

Robbins Schwartz

51

Final
Recommendations
and Risk Mitigation
Strategies

3. Gather and review your district's existing operator agreements to determine what additional provisions may be needed. Pay particular attention to:
 - The scope and types of covered information being shared;
 - Provisions governing data security and breach procedures; and
 - Provisions governing re-disclosure by the operator to third parties or affiliates.

Robbins Schwartz

52

Final
Recommendations
and Risk Mitigation
Strategies

4. Where there is no existing written agreement in place between the district and a particular operator, consider utilizing the NDPA and Illinois exhibit to ensure compliance with SOPPA's written agreement requirements.



Robbins Schwartz

53

Final
Recommendations
and Risk Mitigation
Strategies

5. Review and assess your district's current cyber liability coverage and communicate with operators regarding the scope of their cyber liability coverage.

Robbins Schwartz

54

Final
Recommendations
and Risk Mitigation
Strategies

6. Review and assess your district's security procedures and practices and communicate with operators regarding their security procedures and practices pertaining to covered information.

Robbins Schwartz

55

Questions?



Robbins Schwartz

56

Contact Us:

Matthew J. Gardner

mgardner@robbins-schwartz.com

Emily P. Bothfeld

ebothfeld@robbins-schwartz.com

Tim McIvain

tmclvain@icollinois.org

Chris Wherley

cwherley@icollinois.org

Tyler Mackenzie

Tyler_Mackenzie@ajg.com

Michael McHugh

Michael_McHugh@ajg.com

Will Durkee

wdurkee@securehalo.com

Robbins Schwartz

Robbins Schwartz



Matthew J. Gardner
Robbins Schwartz
Attorney
Chicago, IL

mgardner@robbins-schwartz.com

Matthew J. Gardner is a member of the firm's construction, real estate, and public finance practice groups. Matt represents private and public project owners over the course of construction and development projects, beginning with property acquisition, zoning, contract negotiation and bidding, project management, surety and warranty claims and any resulting litigation concerning payment, delays or design or construction defects. Matt also represents contractors, subcontractors, and suppliers on a variety of construction-related matters, including payment claims, preserving and enforcing lien rights and defending defect claims.



Emily P. Bothfeld
Robbins Schwartz
Attorney
Chicago, IL

ebothfeld@robbins-schwartz.com

Emily P. Bothfeld practices in the area of education law with a focus on student and higher education matters. She counsels school districts and higher education institutions on a variety of issues, including matters related to student discipline, Title IX, free speech, student disability rights, student data privacy and policy development. She has extensive experience representing educational institutions in responding to complaints filed with the U.S. Department of Education's Office for Civil Rights, Illinois State Board of Education, Office of the Illinois Attorney General and Illinois Department of Human Rights. Emily regularly represents school districts and higher education institutions in state and federal court on civil rights and constitutional claims and breach of contract claims



Tyler MacKenzie
Gallagher
Account Executive – Key Accounts
Rolling Meadows, IL
Tyler_Mackenzie@ajg.com

Tyler MacKenzie has been in the insurance industry since 2010. During this time, he has handled complex risk pools with a focus on Public K-12 School Districts. His ability to work with large sets of exposure and loss data produce both an efficiently and effectively run pool program.

Tyler provides strategic risk management consultation to clients while also negotiating coverage placements with insuring partners and reviewing coverage documents for adequacy and accuracy. Tyler's ability to evaluate self-insuring mechanisms have resulted in both premium savings and leverage in the insuring marketplace for his clients.

Tyler has held his Property/Casualty Insurance Producer's license since 2010 in addition to holding the professional designations of *Associate in Insurance Services* and *Commercial Lines Coverage Specialist*.



Michael McHugh
Gallagher
Area Senior Executive Vice
President
Rolling Meadows, IL
Michael_McHugh@ajg.com

Michael McHugh has been in the insurance industry since 1980. During this time, he has been directly involved in the design, implementation, and management of property & casualty and workers' compensation pool programs for public entities nationwide.

Michael was recognized as a Power Broker by *Risk & Insurance* magazine in 2011, 2014, 2016, 2018, 2020 and 2021. Power Brokers are selected annually among thousands of nominees based upon superior customer service, depth of industry knowledge and successes in solving difficult client risk-related problems. He has successfully provided service to more than 700 public school districts and other governmental entities across the nation giving him an in-depth understanding of the needs, concerns, and priorities of school superintendents, business managers, city managers, and governmental officials. In addition, Michael has spoken on numerous occasions regarding insurance issues and educational and public entity topics. He spent a summer internship at Lloyd's of London.

Michael holds a bachelor's degree in business administration from Regis College, Denver. His professional affiliations include Illinois Association of School Business Officials Risk Management Committee Chairman, Illinois ASBO Exhibitors Committee, and Illinois ASBO Services.

LEARNING
TECHNOLOGY
CENTER of ILLINOIS



Chris Wherley
Learning Technology Center
Director of Technology Services
Springfield, IL
cwherley@ltechillinois.org

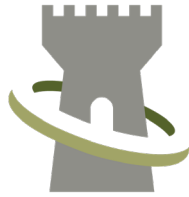
Chris Wherley is the Director of Technology Services for the Learning Technology Center of Illinois (LTC). Prior to joining the LTC, Chris was the Director of Technology at an Illinois K-12 Public School District for 21 years and gained a broad knowledge of technologies such as G Suite, Chromebooks, iPads, networking, wireless, VOIP, servers, and virtualization. He also supported classroom teachers in their use of technology devices and applications. In his role at the LTC, Chris identifies and develops services and resources, provides technical and consultation support, and leads and facilitates professional learning events for Illinois Districts and Schools. Chris has earned COSN's Certified Education Technology Leader (CETL) certification and Amplified IT's G Suite Admin certification. Chris works out of the Sangamon/Menard Regional Office of Education #51 in Springfield, IL.



Tim McIlvain
Learning Technology Center
Executive Director
Champaign, IL
tmcivain@ltechillinois.org

Tim McIlvain directs the Learning Technology Center, the leading Illinois organization that delivers technology and education services to all K-12 schools and districts in the state. He provides strategic leadership, expertise, and operational management for technology and digital learning initiatives. Primary areas of focus include technology infrastructure, personalized and digital learning, data security and student safety, equity and access, and industry and community partnerships.

Tim is a frequent presenter on educational technology topics and serves in leadership roles on several boards and committees. He is a National Board-Certified Teacher, Google Trainer and Administrator, Certified Educational Technology Leader (CETL), and Microsoft Innovative Educator. Before his role as Director, Tim was a teacher, project manager, and web developer.



SECURE HALO

SECURING THE ENTERPRISE



Will Durkee is the director of security services at Secure Halo. He has been with Secure Halo for five years, starting as a security consultant and conducting assessments specifically around physical security and insider threat. He has since obtained his CISSP certification, insider threat program manager and third-party risk management certifications. Will has worked in both large and small firms around the world, including postings in Taiwan, England, and Russia, and focuses on advising firms on risk-based security strategies and cybersecurity best practices.

Will Durkee
Secure Halo

Director of Security Services
Silver Spring, MD
wdurkee@securehalo.com