



Student Data Privacy Consortium



Access 4 Learning
Community

Powered by:  **SIF**

Simple. Secure. Scalable. Standard.

A Model Now Proven

THE FREE/OPEN PRIVACY STANDARD DRIVING RELATIONSHIPS TO COMPLIANCE

SCOTT GALLANT, KEYED SYSTEMS/WEBSHIELD

STEVE SMITH, CAMBRIDGE PUBLIC SCHOOLS

AISH AGRAWAL, HMH CO

MIKE REYNOLDS, CEDAR LABS

AGENDA

- STUDENT DATA PRIVACY CONSORTIUM BACKGROUND
- GLOBAL EDUCATION PRIVACY STANDARD
- MA DATA HUB SERVICES
- EDTECH PROVIDER CHALLENGES
- COMMON REQUIREMENTS, STREAMLINED SOLUTIONS
- Q & A

Student Data Privacy Consortium Background

The SDPC:

- Started in 2015 to address stakeholders data privacy “Pain Points”
- Organized as a Special Interest Group (SIG) of Access 4 Learning Community (a 501c3 Member Tech Standards Organization)
- Maintains its own governance, oversight and resource support
- Has schools, districts, regional and state education agencies, other professional organizations and marketplace providers as members
- Is supported through membership dues



Student Data Privacy Consortium Background

Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management,

Identify **projects that have on-the-ground and real-world impact** on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections,

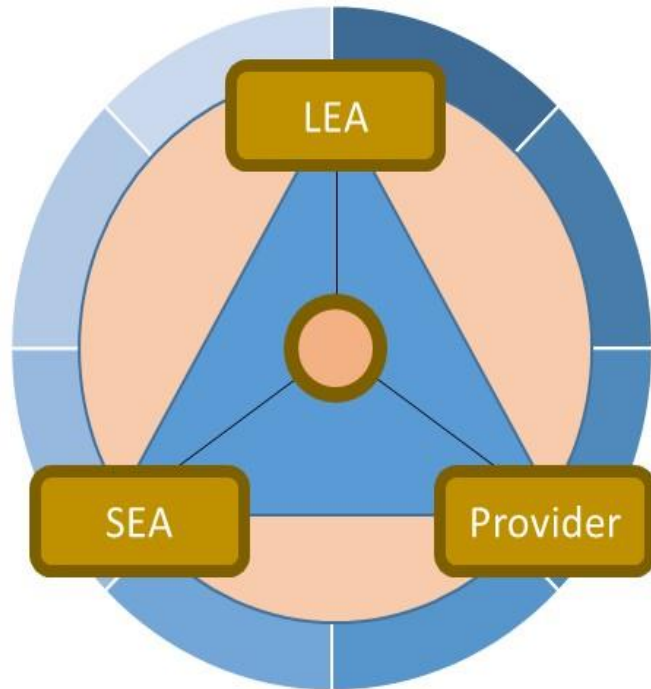
Development of **tools and resources** to address operational issues not currently being addressed,

Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work,

Development of a **clearinghouse of student data privacy operational issues** and resources to support schools, districts, states and vendors in managing those issues – no matter where the resources originate.



Student Data Privacy Consortium Background



-  Consortia sponsored products/tools services
-  Consortia membership, ideals, mission
-  Tangential initiatives and groups, including privacy initiatives, funders, etc
-  Core stakeholder/consumer/client
-  Stakeholder relationship driving core directives through pain points



Privacy By The Numbers

The Student
Data Privacy
Consortium
12/18

26



State-wide Alliances

3



Contract Framework
Digital Tools Governance
Global Education Privacy Standard
Tactical Privacy Projects

32million



Students supported
by Projects

8700+



School Districts
represented

4



Countries Collaborating
on Privacy Issues

4469



Signed Vendor
Agreements

2242



Applications in
Database

3145



Signed "Piggyback"
Exhibit E



Global Education Privacy Standard

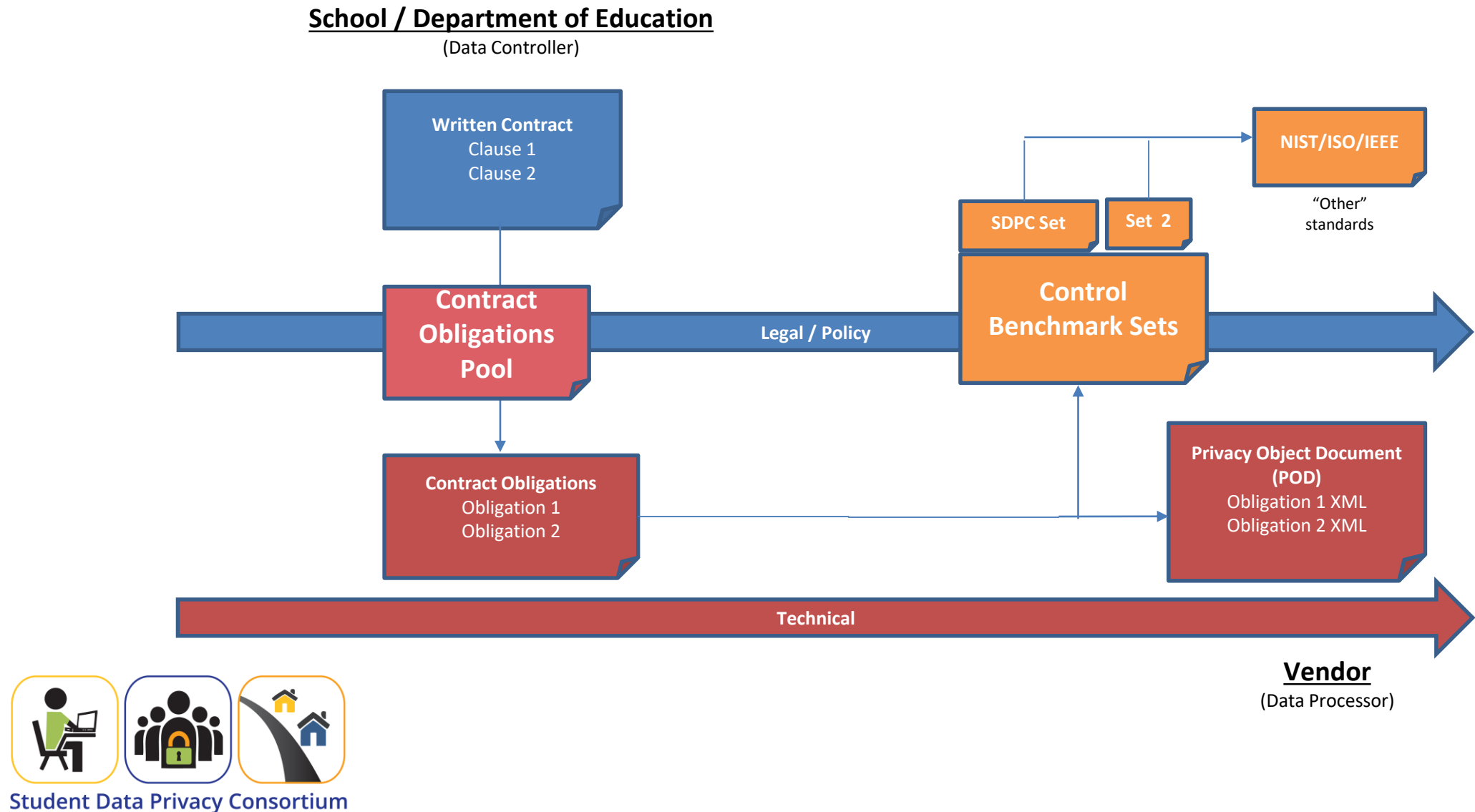
OK the contract is all signed between marketplace provider and customer, the deliverables are clearly outlined and everything is outlined in the roles and responsibilities of each party.

Ready to go, right? No. *In most cases the next call between the two parties to answer the question “How do you want us to deliver on X, Y and Z?”. This is especially true when it comes to student data privacy issues which usually outlines the need for vendors to use “industry established best practices/standards”. The issue is that for the education vertical, no practices or standards exist.*

The Global Education Privacy Standard, GEPS, *is a PK-20 global set of data privacy obligations (obligations) that can be aligned to contractual clauses as well as technical control benchmarks. GEPS includes open XML code (PODS) to transfer privacy obligations between controllers and processors to bridge the gap in understand of education data protection expectations. GEPS allows for organizations to choose the SDPC standard suggestions or use other existing standards, (i.e. IEEE, NIST, ISO, etc.) to set their own expectations between vendors and customers on managing student data.*

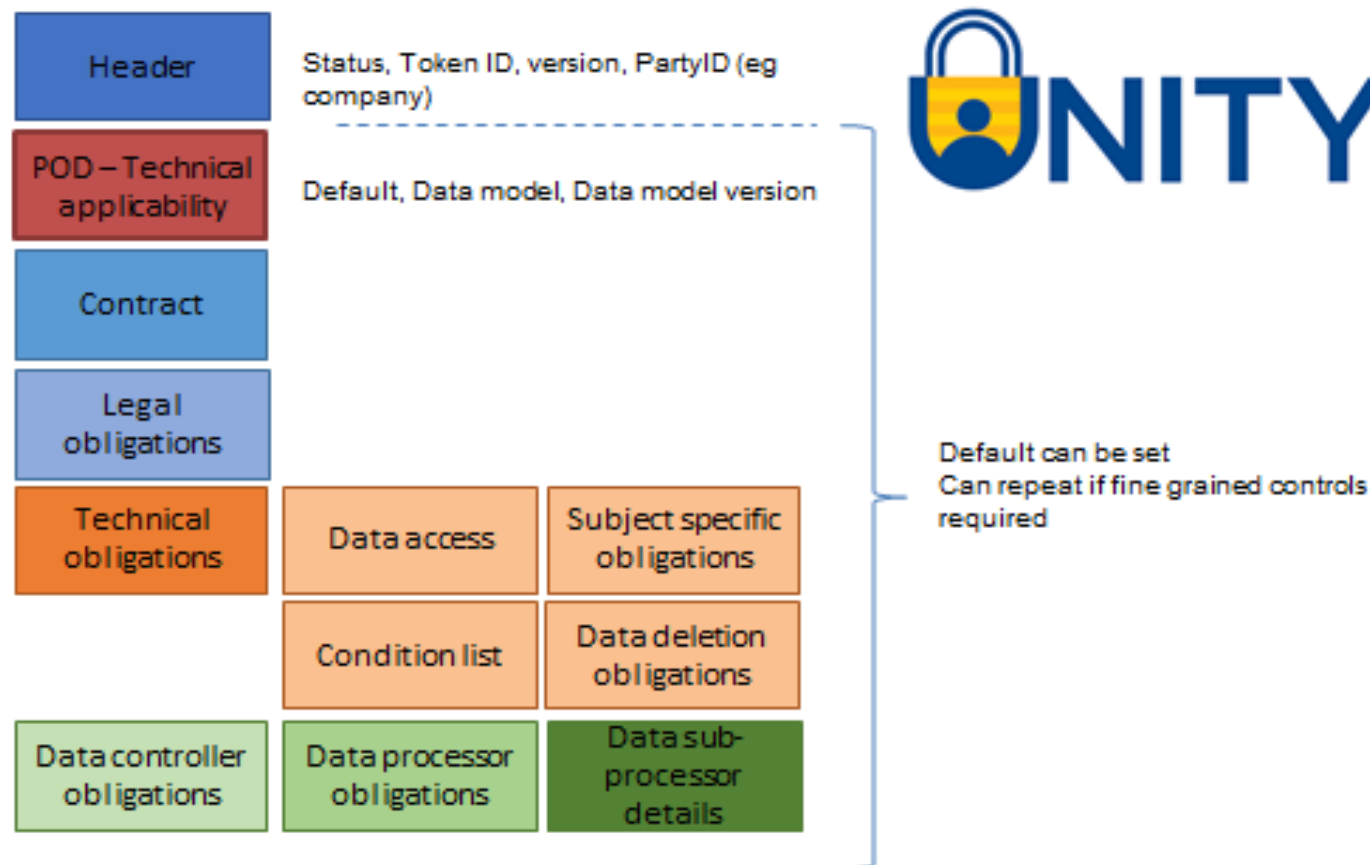


Global Education Privacy Standard



Global Education Privacy Standard

POD contents (SIF Infrastructure)



Global Education Privacy Standard

DEMO

The screenshot shows a web browser window with the address bar displaying <https://sdpc.a4l.org>. The website has a green header with the title "SDPC Resource Registry" and a navigation bar with links: "About the Consortium", "Projects / Initiatives", "Get Involved", "Members and Partners", and "Login".

The main content area features a large banner for the "2019 2nd Annual SDPC Meeting" held on "APRIL 3, 2019 | PORTLAND, OR". The banner lists the following topics:

- Contract Framework Update
- Digital Governance Tool Update
- Workshop on the SDPC Global Education Privacy Standard
- Student Privacy Boot Camp for non-SDPC members

A "Register" button is located to the right of the list. Below the banner, a "Welcome" section is visible.

The page is divided into four columns of content:

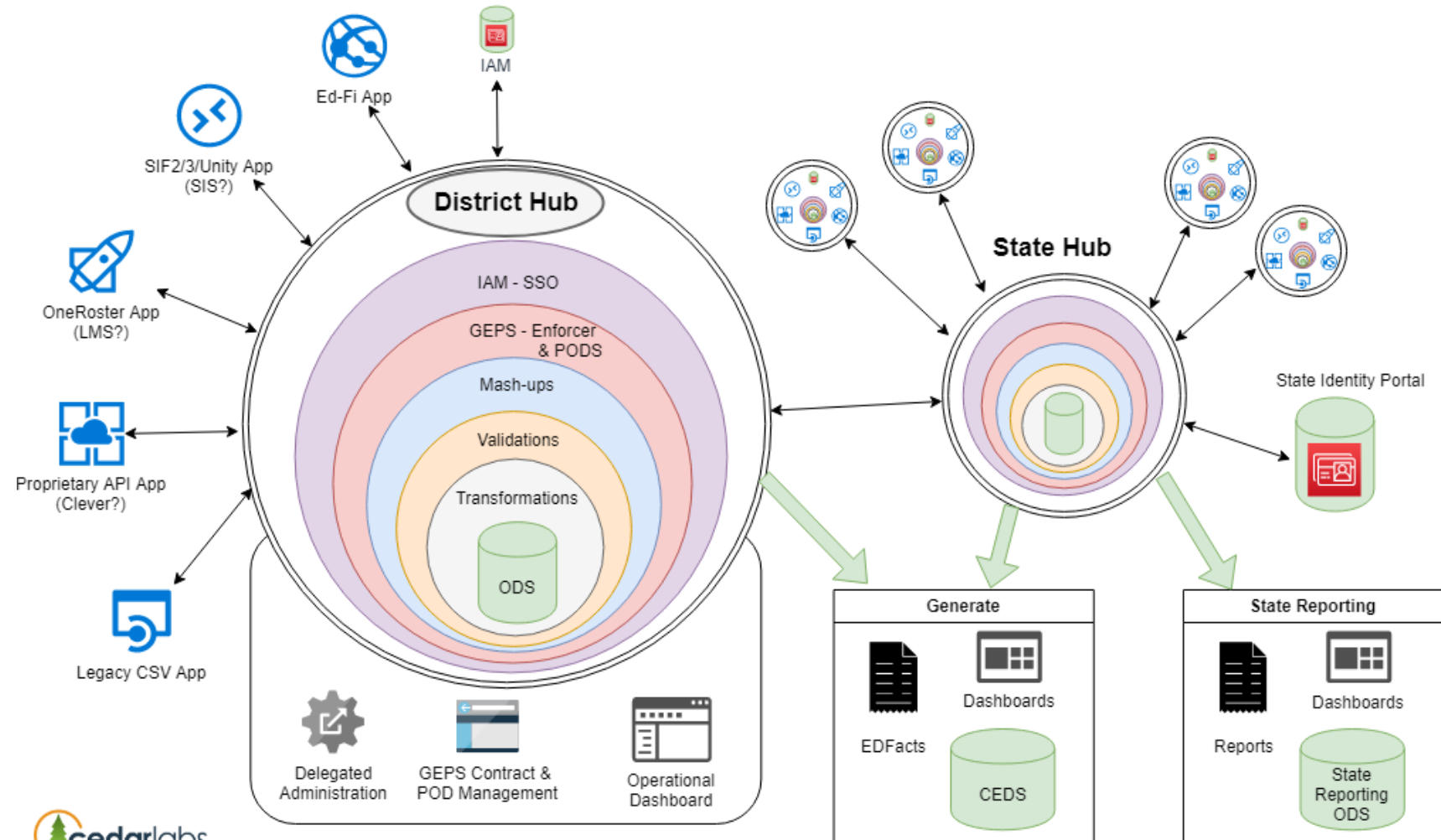
- About SDPC:** A section describing the SDPC as a collaborative of schools, districts, regional, territories, and state agencies. It includes a link to "View Participating Districts" and a "Login" link for existing members.
- State Alliances:** A section with a "Select a State" dropdown menu and a "Visit an Alliance >>" button.
- Search the Database:** A section with a brief description and a "Get started >>" button.
- Quick Stats:** A section titled "Nationwide SDPC Stats" showing the following data:
 - # of Countries Participating: 1
 - # of States Participating: 21
 - # of Districts Participating: 6967
 - # of Vendors Participating: 20
 - # of Resources: 1618

The footer of the website is orange and contains the text "Are your students safe online? Join us!". Below this, there are links for "PAGES" (About the Consortium) and "CONTACT US" (A4L Community).



MA Data Hub Services

MA Data Hub



Student Data Privacy Consortium



Copyright © CedarLabs, LLC 2019 — All Rights Reserved



Market Provider Challenges

- Many to Many contractual relationships
- Use of data is growing across programs and platforms
- Lack of standardization across contracts when it comes to privacy
- Different privacy requirements at State, Regional, District level
- Time and resource intensive to fulfil all these obligations individually
- Prevents a quick and effective turnaround and implementation
- Significant advantage to receiving technical benchmarks over the wire



Common Requirements, Streamlined Solutions

BACKGROUND:

- Orgs lack \$\$ to understand and interpret requirements. *There is knowledge and response gap.*
- Innovation is driving more and more data uses. *The gap is growing faster than we can plug it.*
- Sectoral involvement drives state privacy regulation. *We are not adequately filling this role.*
- Provider tools and services do not scale to all K12. *The cost of compliance is high.*
- People consider data risk in their digital experiences. *Public expectation of trust has changed.*

PROBLEM:

The advent of multiple security/privacy one-pagers, guidelines, laws, and industry solutions led us from barren landscape to the wild west in 6 years. The cost falls to the people, student safety is at risk, and accountable entities need support.



Student Data Privacy Consortium

 Keyed Systems

Common Requirements, Streamlined Solutions

A RECENT KEYED SYSTEMS STUDY

- NH RSA 189:66 (32 clauses)
 - #24: 'department shall establish minimum standards'
 - NH DOE Minimum Standards (44 items)
 - ... with references to NIST 800-171
 - ... a derivation of NIST 800-53
- 9 pages**
125 pages
462 pages!
- Done? NOPE! At least 9 more state laws.
 - And of course federal COPPA/FERPA/PPRA/etc
 - Then any obligations to Privacy Pledge, TLE, or industry initiatives
 - And don't forget parsing through your contracts...
 - SDPC Contract DPA Draft (47 Provisions)



Common Requirements, Streamlined Solutions

A RECENT KEYED SYSTEMS STUDY

- N
-

SDPC Common Contract DPA [draft]

- 47 DPA provisions
- 33 Not covered by NH Minimum
 - 7-8 n/a
 - 2-3 somewhat 'catch all' for the 'standards'
 - Some are direct legalease required not relevant to controls

Minimum Standards for Privacy and Security of Student and Employee Data (NH DOE)

- 44 LEA standard requirements to be implemented by LEAs and Service Providers
 - Due to NIST security origin lacks specific privacy direction for- notices, limited use, subject rights, 3rd party usage and assessments, marketing, research, etc





Home

Components

Catalogs

Classification Schemas

UseCase

Laws / Regulations /
Policies

Controls

Contracts / Agreements

Organizations

Training / Resources

Documents

Reports

Control Framework

Update

Cancel

Control Framework Data

Name* : NIST Special Publication 800-53 Version* : 4

Organization* : National Institute of Standards and Technology Description* : Part of: FISMA is a massive 462-page document that covers the framework that government institutions use for appropriate

Type* : Standard

Owner* : Scott

Long Description :

B I U S           

Font Size Style

security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

This NIST SP 800-53 database represents the security controls and associated assessment procedures defined in NIST SP 800-53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations. Any discrepancies noted in the content between this NIST SP 800-53 database and the latest published NIST Special Publication SP 800-53 Revision 4,

NIST Special Publication 800-53

CM - Configuration Management

CP - Contingency Planning

+ IA - Identification and Authentication

- IR - Incident Response

Control Objective

Update

Cancel

Name* : IR-4 INCIDENT HANDLING

Description* : Supplemental Guidance Organizations recognize that

Identifier* : IR-4

Domains : Notice, Incident Response and Recovery

NIST Special Publication 800-53

CM - Configuration Management

CP - Contingency Planning

+ IA - Identification and Authentication

- IR - Incident Response

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

IR-2 INCIDENT RESPONSE TRAINING

IR-3 INCIDENT RESPONSE TESTING

- IR-4 INCIDENT HANDLING

a. Implements an incident handling capability for security incidents that includes preparation, detecti

b. Coordinates incident handling activities w contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response pro

IR-5 INCIDENT MONITORING

IR-6 INCIDENT REPORTING

IR-7 INCIDENT RESPONSE ASSISTANCE

IR-8 INCIDENT RESPONSE PLAN

Control Objective

Update

Cancel

Name* : IR-4 INCIDENT HANDLING

Description* : Supplemental Guidance Organizations recognize that

Identifier* : IR-4

Domains : Notice, Incident Response and Recovery

Categories : Procedural

Label* : Objective

Types : Corrective

Priority : Select Priority

Similar Objectives : Select Similar Objectives

Controls : a. Implements an incident handling

Control

Update

Cancel

Name* : b. Coordinates incident handling :

Description* : b. Coordinates incident handling activities with

Identifier* : b.

Domains : Sharing & 3rd Party, Systems and Application Security, Breach Notification

Categories : Physical

Types : Preventive, Detective

Edspex Introduction

OPPORTUNITY

Support districts/vendors protect people by maintaining a proprietary framework of security/privacy expectations leading to our best-practice and marketplace solution.



Student Data Privacy Consortium

Edspex Introduction

OPPORTUNITY

Support districts/vendors protect people by maintaining **an open** framework of security/privacy expectations leading to best-practice and marketplace solutions.



- **Affirm our responsibility:** Safety/Protection of Students
- **Build knowledge and response:** Privacy & Security Content
- **Use our best capability :** Community



Student Data Privacy Consortium

Edspex Introduction

Get Engaged...

www.edspex.com

(Workgroup calls every other week)
(Webinar training event early Sept)



Edspex



Fagen Friedman & Fulfrost LLP



Keyed Systems



Student Data Privacy Consortium



WEBSHIELD



EP3 FOUNDATION



Edspex Introduction



- An attainable set of control guidelines
- Alignment to industry & external models
- Addressing requirements for all states
- Room for local loosening or tightening
- Supportive of a maturity model over time
- Security and Privacy
- Agency and Provider
- Support of a Community.



Questions



Student Data Privacy Consortium