
PCI
CLICK, AGREE, COMPLY
SURVIVING EDTECH ADOPTION
IN THE AGE OF HB55
NotebookLM

I.T. Signed What?! ?!

EdTech Contracts for K–12 Humans

(A Survival Guide for the Age of H.B. 55)

Angela Thompson
North Sanpete School District
UETN Tech Summit 2026

You Didn't Ask For This Job... But Here We Are.

What You Were Hired To Do

- ☐ Manage devices and networks
- ☐ Reset Chromebooks
- ☐ Fix the Wi-Fi
- ☐ Support learning standards

What You Actually Do Now

- Manage legal data flows
- Defend student privacy (FERPA, HB 55)
- Decode 40-page Terms of Service
- Last Line of Defense

The Three Worlds Colliding at 2:15 PM on a Tuesday

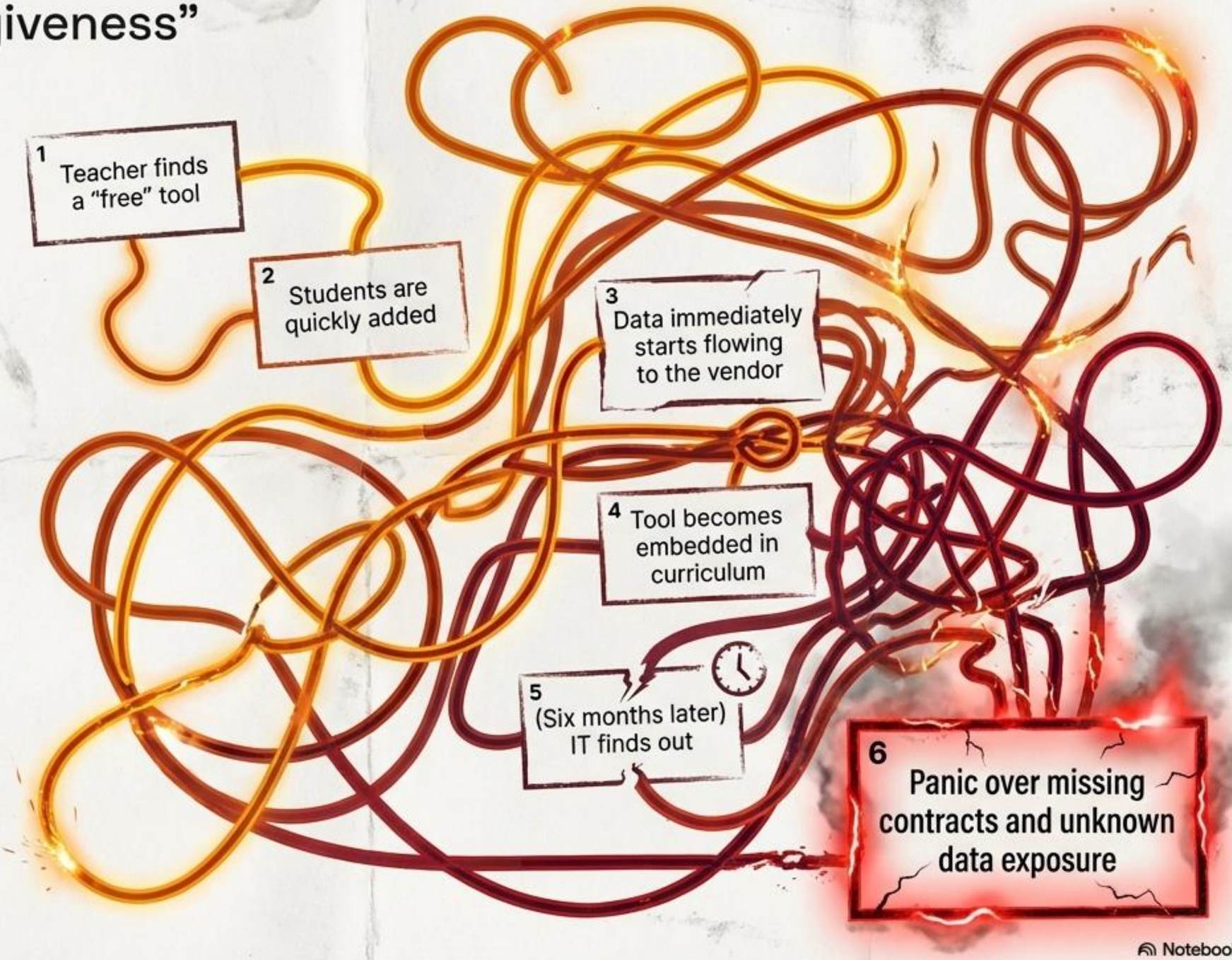
USBE tells you what process to follow.	HB55 dictates why it matters legally.	District reality demands speed and frictionless access.

The Broken “Ask Forgiveness” Deployment Model

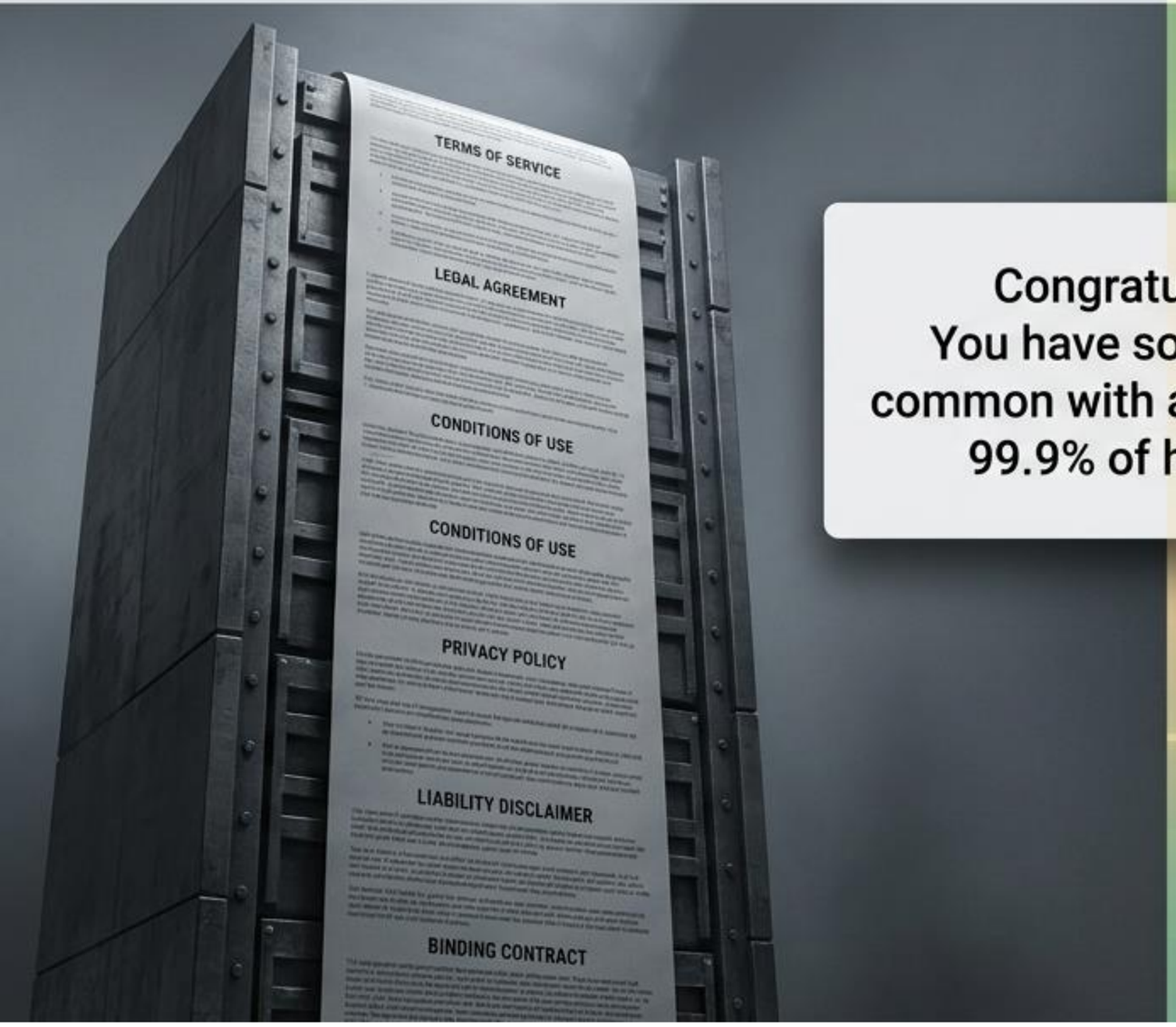
This is the most common EdTech deployment model in America.

It is driven by enthusiasm, not procurement.

The result: Mission-critical apps operating with no contract and no exit plan.



Almost everyone has clicked ‘I Agree’ without reading the Terms of Service.



Congratulations.
You have something in common with approximately 99.9% of humanity.

The rules for digital classrooms have fundamentally changed.

Student Data Privacy.
Strict enforcement of HB 55 (2026) regulations.

Vendor Oversight.
Strict liability for third-party agreements.

Artificial Intelligence.
The explosion of generative LLMs and algorithmic bias.

Instructional Purpose.
Required screen-time expectations and proven educational ROI.

The days of “everybody else uses it, so it must be fine” are officially over.

You Are Now the Gatekeeper of Data Systems

Approving an App

Approving a Data System

Every Click = A Vendor Relationship + A Data Flow + A Compliance Obligation

EdTech is no longer optional; it is embedded infrastructure.

Every single tool involves data collection.

Every approval is a formal risk decision for the district.

HB55 Translated into Plain English

Must have strict contracts aligned with FERPA, GRAMA, and GDPA (63A-19).

Must explicitly define data use and allow district audits.

Must be able to mandate and verify data deletion.

Must have the right to terminate without penalty for privacy violations.

- You must know exactly what data is collected.
- You must know exactly where it goes.
- You must be able to walk away instantly if the vendor breaches trust.

This is Not a Data Buffet

What the app asks for.

What the app actually needs.

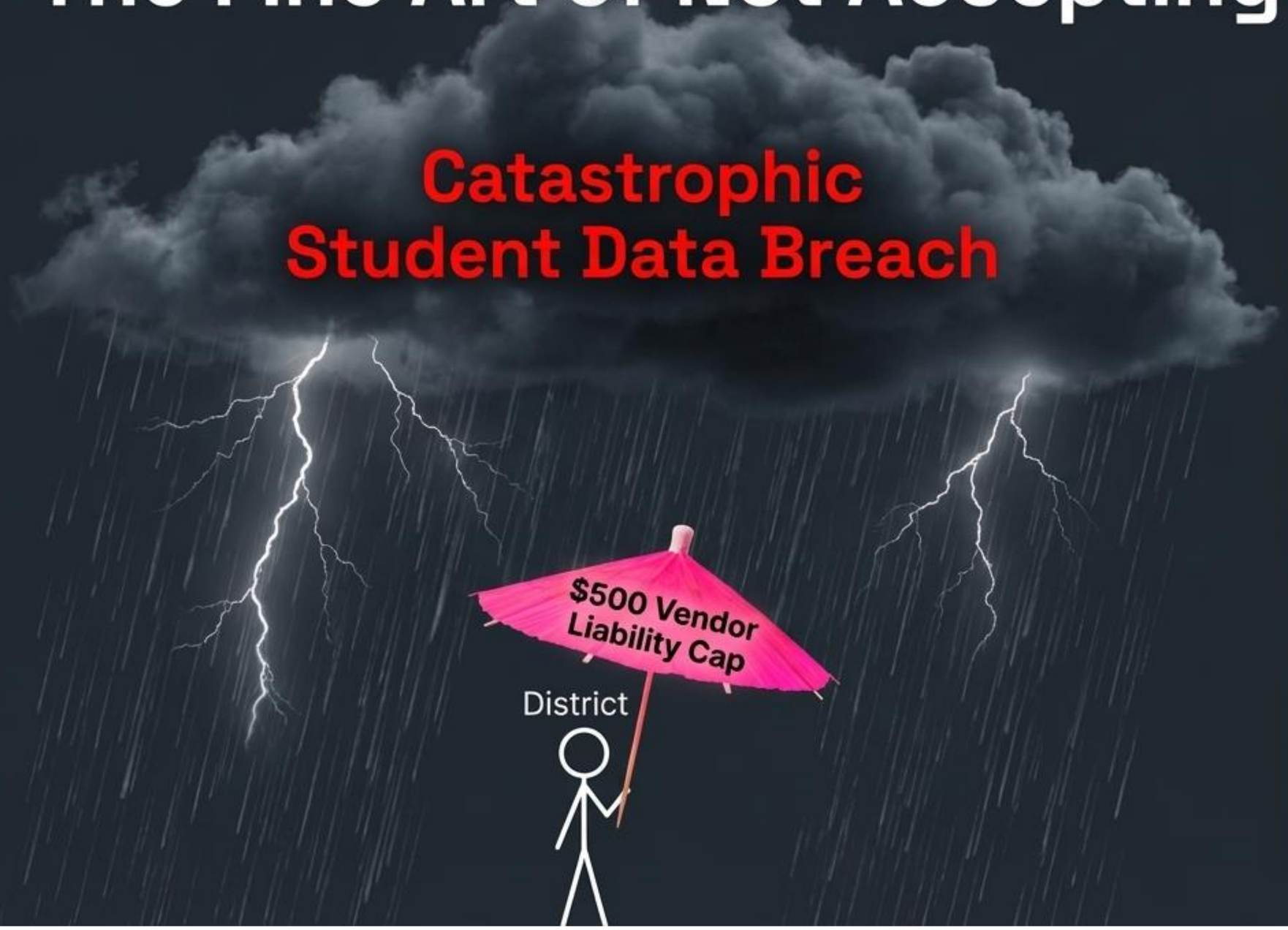
- Vendors should only collect data strictly necessary for the service.
- Beware of “optional” fields that aren’t actually optional.
- Beware of requests for full student records for a simple spelling app.

Stay in Your Lane with Purpose Limitation

Used to deliver assessments and generate progress reports.

Used to enhance user experience or Shared with trusted partners.

The Fine Art of Not Accepting All the Risk



Vendors frequently attempt to limit liability to the amount paid (often $0 for free apps).

HB55 demands real accountability—no hiding behind tiny caps.

You must demand no limits for data breaches, legal violations, or confidentiality failures.

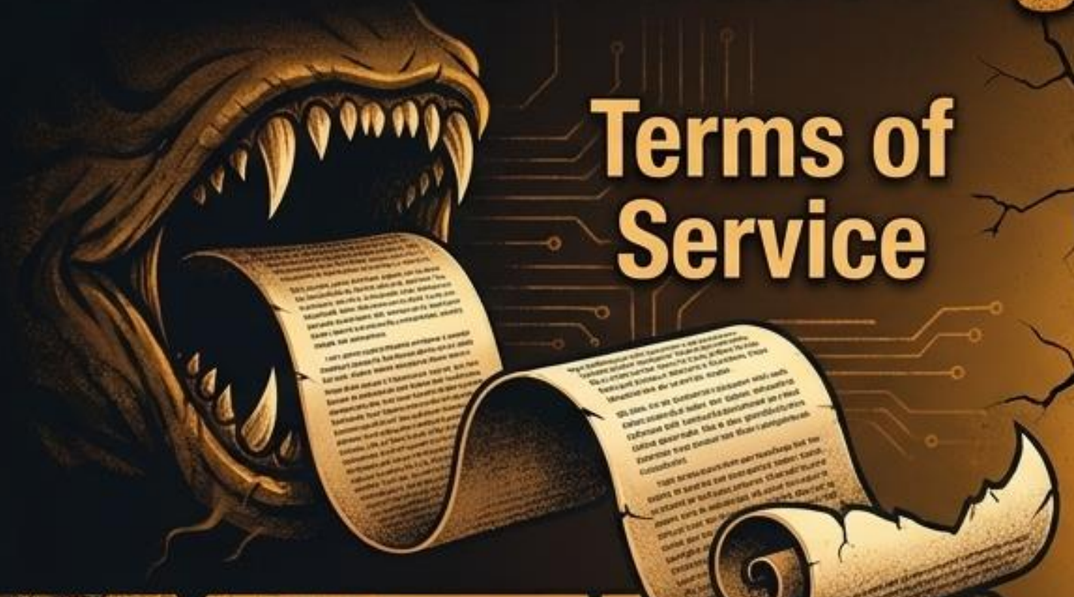
Deletion is Verified, Not Assumed

HB55 requires **defined retention** and **secure deletion** upon contract termination.

Account **deprovisioning** must be **immediate**.

You must require the vendor to provide **proof/certification** of **deletion**.

The Fine Print Fight Club: ToS vs. DPA



Terms of Service

Signed DPA

The Problem

"Nobody reads the Terms and Conditions." But when a predatory standard Terms of Service collides with a highly protective Data Privacy Agreement, you have a legal disaster.

The Reality

A contract is only as strong as its weakest document. If their own documents contradict each other (e.g., one says "no sharing", the other says "we may share with partners"), district liability skyrockets.

The Analogy: Relying on a DPA while letting staff accept a predatory ToS is like putting a seatbelt on after you've driven the car into the lake.

The Addendum operates as the ultimate legal referee.

The Addendum is a formal, signed instrument that acknowledges both documents but establishes absolute supremacy over the ecosystem.

The Golden Clause

In the event of any conflict between the vendor's Terms of Service and the District Data Privacy Agreement, the strict terms of the DPA shall exclusively govern.

The Red Flags Cheat Sheet

Green Flags (Proceed)	Red Flags (Pause/Reject)
Data used strictly for educational purpose.	We may use data to improve services.
District retains full ownership of data.	We may share with trusted partners.
Automatic deletion upon contract termination.	Liability capped at amount paid by district.

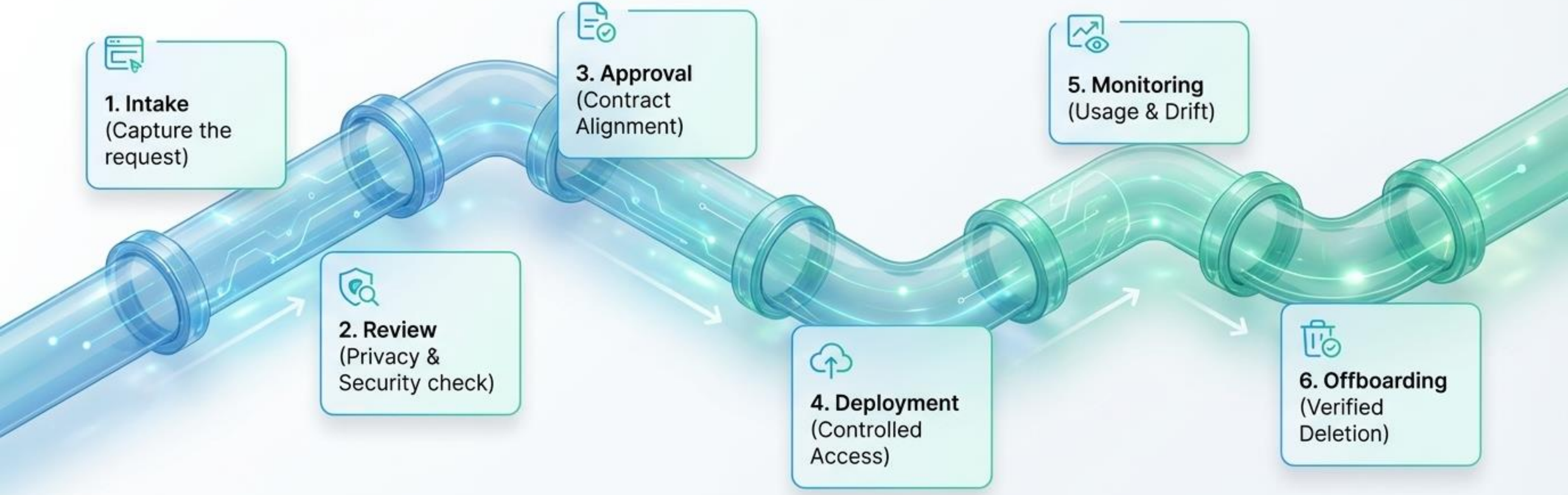
You don’t need to read every word. You need to read the right words.
If it feels vague, it is legally risky.

The Vendor Reality Check Matrix

Vendors are optimized for:	Districts are optimized for:
Speed & Frictionless Signup	HB55 & FERPA Compliance
Viral Growth (Teacher-to-Teacher)	Public Accountability & Trust
Upselling & Monetization	Student Safety & Data Security

Vendors are not evil; their goals just differ from ours.
This tension is why structured governance is mandatory.

Transitioning to the Clean Pipeline



- Move from ‘Click & Hope’ to ‘Structured Governance.’
- Every request follows a visible, accountable path.
- AppTrack enables this exact workflow directly within your launchpad.

Compliance is a Shared Ecosystem

Teachers	Request tools & use them responsibly.
IT	Technical review, interoperability, & enforcement.
Records/Data Privacy	Contract alignment & HB55 compliance.
Administration	Final approval authority & budget.

- **Approval = Responsibility.**
- **Stop being the accidental lawyer**; distribute the load.

The Intake Friction Funnel

I saw this on Facebook, let's use it!

Instructional Justification:
Does this solve a specific curriculum standard, or is it just shiny?

Data Classification:
Does this require Directory Info? PII? Behavioral data?

Technical & Legal Readiness:
Will it sync with our SSO? Is there a privacy policy?

Slow the process down just enough to make it safe. A required intake form exposes whether an app is essential or an impulse buy.

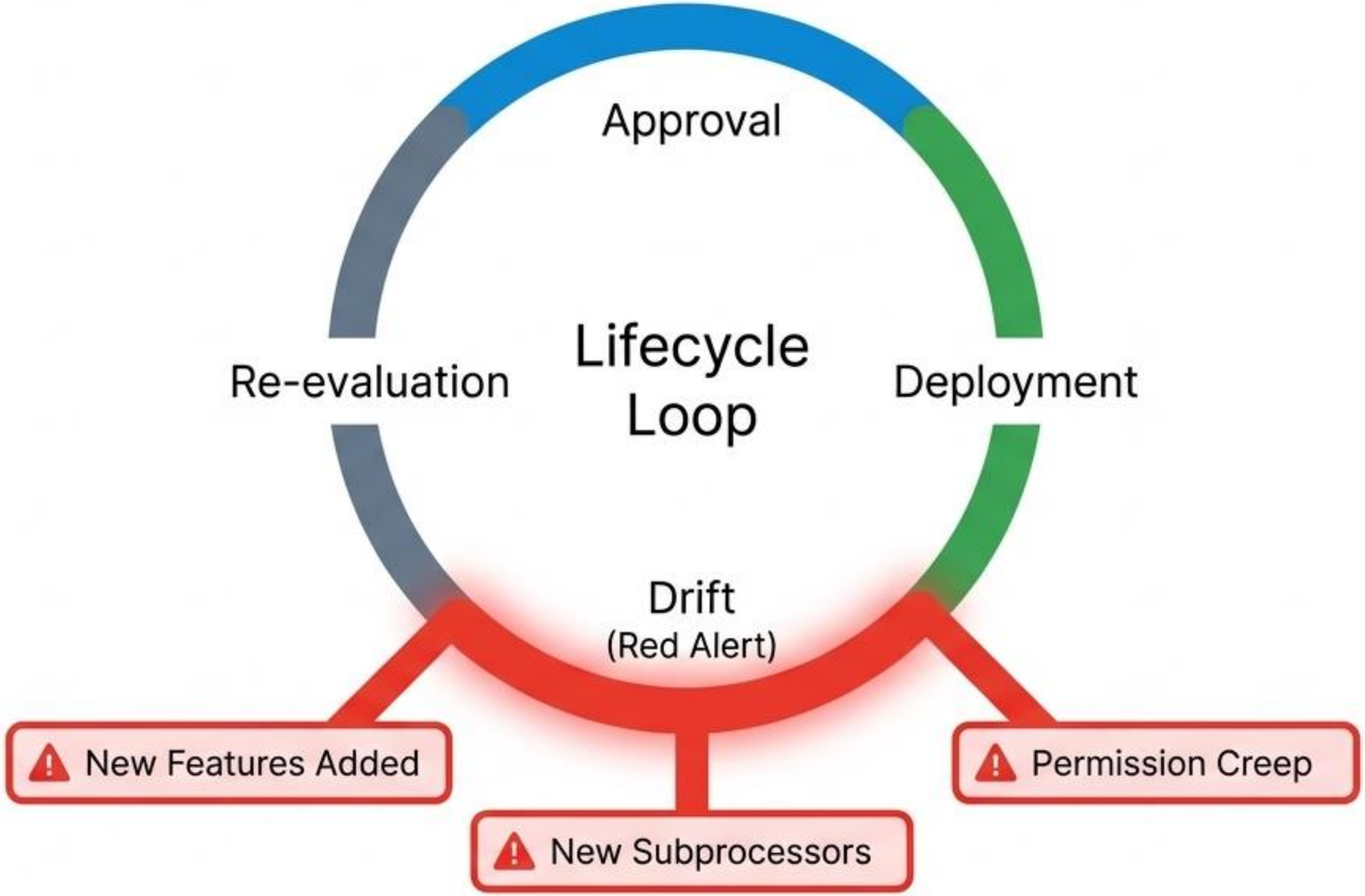
Vetted, instructionally sound, compliant apps.

The Most Dangerous App is the One You Forgot About

A compliant tool today can be noncompliant next semester.

Watch out for silent updates to Terms of Service.

Require an annual review for all integrated tools.



THE ILLUSION

Theoretical Compliance

(You did everything right)

THE REALITY

Monday Morning Reality

(The data is exposed anyway)

A Signed HB55 Contract Doesn't Prevent a Breach—It Just Dictates the Fallout

The law tells you what happens after a breach. It is up to you to survive it

Funding the Front Line: You Can't Terminate What You Can't Technically Prove

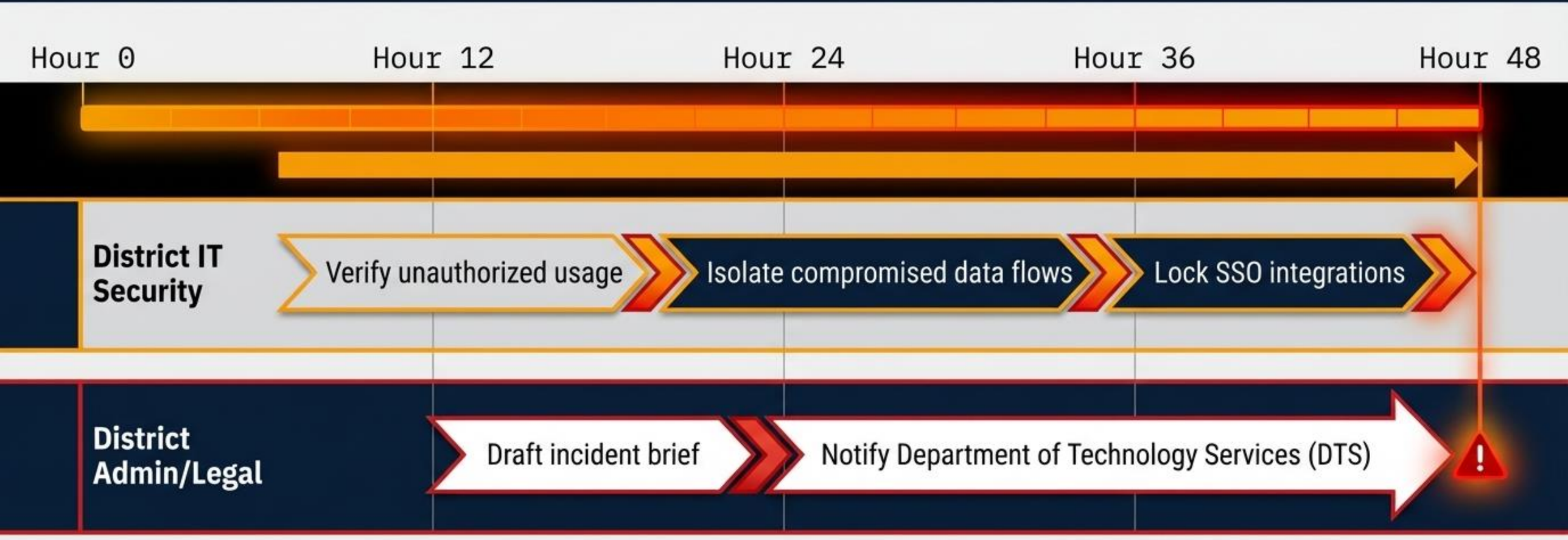
Analytics & Auditing
Track domain-level web browser usage to spot unapproved data exfiltration.

Threat Detection
Actively catch exposed accounts and unauthorized usage.

Track anomalous provisioning.

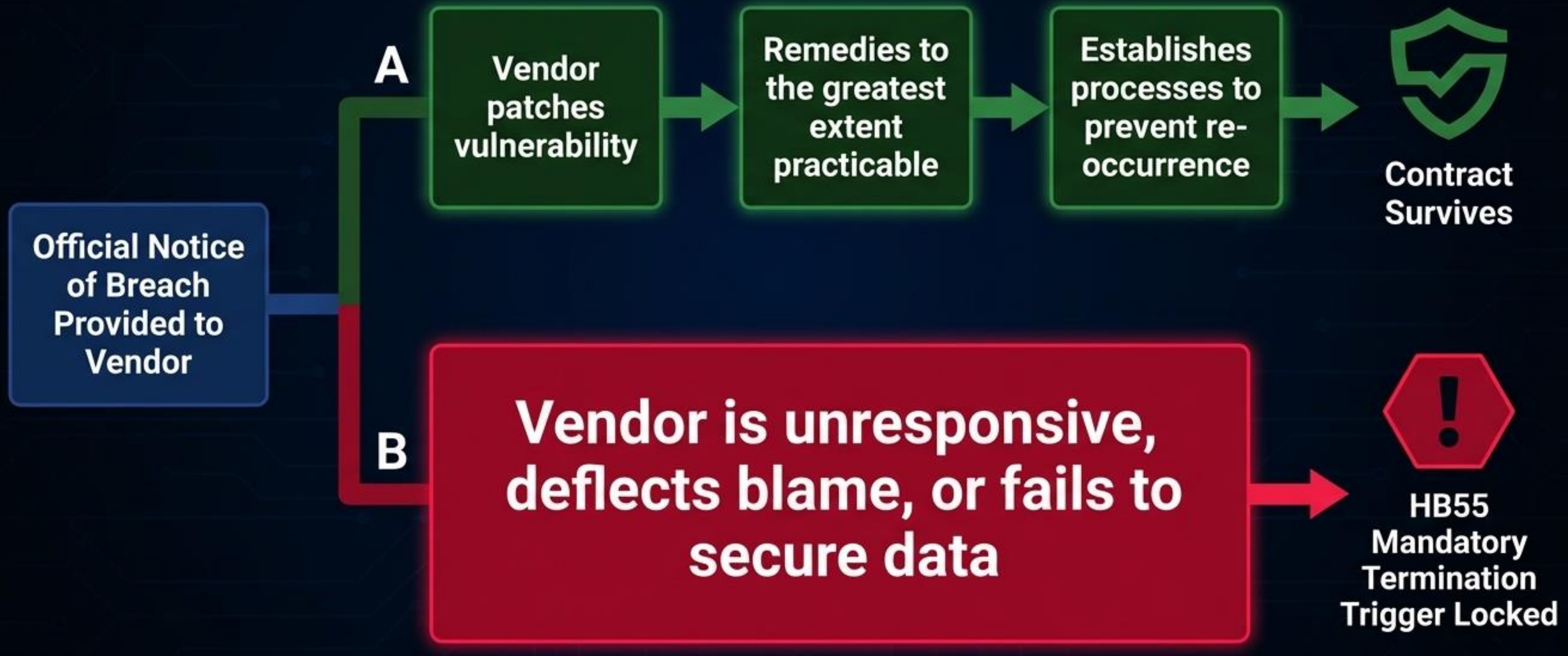
The cost of breach discovery tools is the hidden tax of HB55 compliance.

T+00:00 to T+48:00: The State Notification Sprint



STRATEGIC INSIGHT: Do not fight this alone. Hitting the 48-hour DTS notification window isn't just about compliance; it unlocks state-level Incident Response resources and limits district liability.

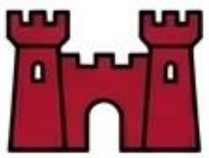
The 30-Day Pressure Cooker: Remedy or Terminate



The Vendor Negotiation Matrix During the 30-Day Window

Vendor Technical Competence (Low to High)

The Hostile Fortress



Technically secure but hides behind lawyers, refusing to admit unauthorized usage.

The Partner

Rapid patch deployment, transparent forensic logs.

The Ghost

Unresponsive.
Immediately prepare for forced termination.

The Apologetic Mess

Wants to help, but lacks the infrastructure to prove data deletion.

X-Axis: Vendor Legal Cooperation (Low to High)

Hope is Not a Strategy: Mapping HB55 to IR & DR Plans

Theoretical Compliance
(Checking the HB55 Box)

- Signed Data Privacy Agreement
- NDPA Addendum attached
- Liability Caps verified

Operational Survival
(IR & Disaster Recovery Integration)

- Pre-identifying backup vendors
- Testing data export formats
- Budgeting for mid-year crisis migrations

You cannot wait until Day 29 of the remediation window to figure out how to replace a core system.

Updating Incident Response Workflows for the HB55 Clock

	Pre-Breach	48 Hour Window	30 Day Window	Day 31
IT Security	Deploy ThreatScan & Analytics →	Forensics & Log Lockdown →	Verify vendor patches	
Legal/Admin		DTS Notification →	Track statutory cure window →	Execute termination
Curriculum/ Instruction		Assess instructional impact →	Source alternative tools →	Deploy emergency replacement

Quick Wins for Monday Morning

- Standardize your Intake Form (Require instructional justification)
- Publish an Approved Tools List (Publicly visible, reducing redundant requests)
- Centralize Contract Storage (Stop relying on email attachments)
- Enforce the Golden Rule: No approval = No technical deployment

You can fix the majority of your risk in a single quarter. Start by halting the bleeding of the “ask forgiveness” model.

The Hidden Mass of the Cultural Iceberg

Technology & Software
(AppTrack, Launchpad, Intake Forms)

Process, Communication, and Managing Teacher Expectations

This is **not an IT problem**; it is a **cultural shift.**

Transparency is key to ensuring adoption.

Expect **pushback**, but lean on the law (HB55) as your shield.

You’ve Got This. (Seriously.)

Your job isn’t to kill innovation. It’s to make sure innovation doesn’t accidentally violate federal law.

- ☐ Be Curious.
- ☐ Be Skeptical.
- ☐ Be Consistent.

Approval = Responsibility

The risk is not that a teacher uses a new app. The risk is that the district cannot explain—after the fact—why it allowed it.

If you approve it, you own it. Not IT. Not the vendor. The district.

The ultimate goal? Good process makes compliance boring.
And boring is exactly what we want.