Data Security Incident and Breach Notification Policy

Think Tech Solutions, Inc.
Think Tech legal and district documentation set

This policy describes Think Tech's external-facing framework for identifying, assessing, containing, remediating, and communicating Data Security Incidents affecting the Services. It is intended to supplement, and not replace, internal incident-response procedures, customer contracts, and district-specific breach obligations.

1. Scope and definitions

"Data Security Incident" means an actual or reasonably suspected unauthorized access to, acquisition of, use of, disclosure of, loss of, or interference with Personal Information, Customer Data, Student Data, or the systems that store or process such data.

"Confirmed Breach" means a Data Security Incident that Think Tech determines constitutes a reportable breach, unauthorized release, or other legally significant event under applicable law, contract, or district-specific obligations.

"Customer" means the Educational Institution, Educator, or other contracting entity that controls the affected Customer Data.

2. Detection, triage, and containment

- Think Tech uses logging, monitoring, user reports, vendor notifications, and internal escalation channels to identify suspected incidents.
- Suspected incidents are triaged to determine affected systems, data categories, users, likely root cause, severity, and whether immediate containment is required.
- Containment steps may include credential rotation, access suspension, feature disablement, session invalidation, patching, network controls, or coordination with service providers and forensic support.
- Think Tech preserves relevant evidence as appropriate, including logs, access records, alerts, tickets, and investigative notes.

3. Customer notice

If Think Tech confirms a breach or unauthorized release involving Customer Data, Think Tech will notify the affected Customer without unreasonable delay after taking the steps reasonably necessary to assess the scope of the incident, contain the threat, and determine the nature of the affected data. Notice timing may be accelerated where contract or law requires a shorter deadline.

To the extent known at the time of notice, Think Tech's notification will generally include:

- a general description of what happened and the date or estimated date of the incident and discovery;
- the categories of affected data and, if known, the categories of affected individuals;
- the containment, mitigation, and remediation steps taken or planned by Think Tech;
- information reasonably necessary to help the Customer meet its own legal, contractual, or regulatory obligations; and

- a contact point for follow-up coordination.

4. New York Education Law § 2-d and Part 121 coordination

For New York Educational Institutions, Think Tech will cooperate with the Customer so the Customer can meet its obligations under Education Law § 2-d and 8 NYCRR Part 121. Where Think Tech is acting as a third-party contractor under that framework, Think Tech's policy is to notify the affected educational agency in the most expedient way possible and without unreasonable delay, and no later than seven calendar days after discovery of a covered breach or unauthorized release involving protected student, teacher, or principal data.

Think Tech will also provide information and cooperation reasonably needed so the educational agency can report the incident to NYSED's Chief Privacy Officer within the agency's 10-day reporting window and can provide affected-parent / eligible-student / teacher / principal notices within the applicable time frame, which is generally no more than 60 calendar days absent a permitted delay.

5. Law enforcement, confidentiality, and delayed notice

Think Tech may delay portions of a notice if law enforcement requests a delay, if immediate notice would materially impede containment or investigation, or if disclosure would create additional risk by revealing an unremediated vulnerability.

Where permitted, Think Tech will provide interim information once it is safe and appropriate to do so.

6. Remediation and post-incident review

After containment, Think Tech seeks to remediate root causes, monitor for recurring activity, evaluate whether policies or controls should be strengthened, and document lessons learned.

Where applicable, Think Tech may update security controls, vendor requirements, product behavior, or training based on the incident review.

7. Contacts

Security incident reports & general privacy or contract coordination: hello@thinktechsolutions.org