Notification Obligations

IR Packet

Client Company — reporting duties likely triggered by a breach, given your sector, location, and data types

Generated: **2026-08-25 14:32** Basis: **K-12 Education · Nebraska · student records, staff PII, financial data · no CUI/FCI**

Decision support, not legal advice. This checklist is composed from your organization profile so counsel and leadership start from the right list instead of a blank page. Deadlines and applicability must be confirmed with your attorney and cyber-insurance carrier — statutes change, and facts of the incident control what actually applies.

Likely obligations, ordered by clock

OBLIGATION	CLOCK	TRIGGER	NOTES FOR THE FIRST CALL WITH COUNSEL
Cyber-insurance carrier notice	Often 24–72h	Policy terms — usually any suspected incident	Late notice can jeopardize coverage, and most policies require using panel counsel/forensics. Call the carrier hotline before engaging outside vendors.
Nebraska breach notification Neb. Rev. Stat. §§ 87-801 to 87-807	Without unreasonable delay	Unauthorized acquisition of unencrypted personal information of Nebraska residents	Notify affected residents; the Nebraska Attorney General must be notified no later than the residents. Encryption safe-harbor may apply — document what was encrypted.

FERPA / student records U.S. Dept. of Education guidance	No fixed statutory clock	Disclosure of personally identifiable information from education records	FERPA sets no breach deadline, but ED guidance expects recording the disclosure in each affected student's file and evaluating notification. State student-privacy laws may add duties.
Law enforcement / information sharing FBI IC3, CISA, MS-ISAC	Recommended, not mandated	Any significant incident	As a public K-12 entity you are SLTT: MS-ISAC offers no-cost incident support. FBI/CISA reporting can assist with decryptor availability and is looked on favorably by insurers.
Payment card brands / bank PCI DSS contractual	Per merchant agreement	Only if cardholder data environment affected	You process limited payments (lunch accounts, activity fees). Confirm early whether the CDE is in scope — it changes the vendor list.

Checked and not triggered for your profile

OBLIGATION	WHY IT DOES NOT APPLY
DFARS 252.204-7012 — 72-hour DIBNet report	No CUI/FCI declared in your organization profile and no CMMC framework subscription. If you ever handle defense contract data, this becomes a hard 72-hour clock.
HIPAA Breach Notification Rule	No PHI declared; the organization is not assessed as a covered entity or business associate. School health records generally fall under FERPA, not HIPAA.

Other states' breach statutes	Only Nebraska is on file as an operating location. If affected individuals reside in other states (staff, transfers), each state's statute applies — raise this with counsel early.

Prepared fields for the notifications you may need to send

- Organization legal name and point of contact (from your profile)
- Data types potentially involved: student records, staff PII, financial
- Population estimate: enrollment + staff counts (confirm during scoping)
- Security measures in place at time of incident: attach the Responder Brief from this packet as the supporting snapshot

---