

FrameworkMapper · Incident Response Packet

Incident Response Packet

Client Company — K-12 Education, Nebraska

Generated: 2026-08-25 14:32 Source assessment: CIS Controls v8.1, completed 2026-08-14 (check-in #2)

Packet fingerprint: 7C4E-91A0-D2B8-3F55

If you are reading this during an incident

- Start with the **Responder Brief** — it tells your response team what this environment is and which security capabilities they can rely on.
- Open **Notification Obligations** within the first hours — the insurance-carrier clock is usually the shortest.
- Use the **Kill-Chain Gap Overlay** once observed attacker techniques are known; the live version in the portal accepts the incident's technique list.
- Hand **Tool KEV History** to whoever is forming the initial-access hypothesis.

Contents

01 Responder Brief

Environment snapshot: identity provider, data types, staffing, and assessed capabilities with the evidence behind each status.

02 Kill-Chain Gap Overlay

Sample ransomware scenario mapped against assessed control coverage; containment actions split by what this organization can actually execute.

03 Tool KEV History

Inventoried products with confirmed Known Exploited Vulnerabilities history — a triage ordering, not a vulnerability scan.

04 Notification Obligations

Reporting duties likely triggered by a breach for this sector, location, and data profile, ordered by deadline.

05 Evidence Bundle (companion ZIP)

Every evidence file submitted during the assessment and its check-ins, one folder per control, with a hash-verified index. Shipped as a separate download — share the reports freely; share raw evidence deliberately.

06 Remediation Crosswalk — reserved

Arrives with the capability question bank: post-incident findings mapped to every framework you maintain.

Custody and freshness

This packet is generated from your organization's own FrameworkMapper data and is **encrypted with your organization key** while stored on the platform. The downloaded copy in your hands is unencrypted by design — it exists so responders can read it when your identity provider, and therefore the portal, may be unreachable or contested.

Keep it where your incident response plan lives: printed in the break-glass binder, or on storage that is not domain-joined. Treat it as sensitive — it describes your gaps as well as your strengths.

The packet regenerates whenever the data feeding it changes (assessment save or check-in, tool inventory update, organization profile edit). Compare the generation date above against your last significant change; re-download after each assessment cycle.

Produced deterministically by FrameworkMapper from data entered by Client Company. Contents are decision support reflecting self-assessed posture as of the basis date — not forensic findings, and not legal advice.