

Responder Brief

IR Packet

Client Company — environment snapshot for incident responders

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

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

Organization at a glance

FACT	VALUE	RESPONDER RELEVANCE
Sector	K-12 Education	Student records in scope; FERPA and state breach law apply — see Notification Obligations report.
Location	Nebraska, US	Nebraska breach statute governs resident notification.
Size / staffing	Small; 3 IT staff, no dedicated security staff	Assume no in-house forensic capability; IT staff double as incident handlers.
Identity provider	Microsoft Entra ID	Account disablement, session revocation, and sign-in logs live here. If attacker holds admin, this console may be contested.
Email platform	Microsoft 365	Message trace and purge available via M365 admin/Defender portals.
Data types held	Student records, staff PII, limited financial	No CUI/FCI declared — defense-industrial reporting clocks do not apply.
Environment	Cloud SaaS-heavy, some on-prem servers; remote workforce: partial; BYOD: yes; internet-facing services: yes	Expect a hybrid estate; on-prem AD-joined servers plus M365 cloud tenancy.

Third parties	~12 vendors with system access	Vendor access review belongs on the containment checklist.
---------------	--------------------------------	--

Assessed security capabilities

Each status is derived from the organization's most recent CIS v8.1 assessment scores. The basis line shows exactly which controls and scores produced the status — treat these as the organization's own attestation, verified where noted, not as forensic ground truth.

CAPABILITY	STATUS	WHAT A RESPONDER CAN RELY ON
Endpoint protection / EDR Basis: CIS 10.1 (4/4), 10.2 (4/4), 10.7 (3/4)	In place	Centrally managed anti-malware with behavioral detection on workstations and servers. EDR console is a viable containment lever (host isolation).
Asset inventory Basis: CIS 1.1 (4/4), 1.2 (3/4)	In place	Current asset inventory exists with owner and network address. Scoping "what machines exist" should be fast.
Multi-factor authentication Basis: CIS 6.3 (4/4), 6.4 (3/4), 6.5 (2/4)	Partial	MFA enforced on externally exposed apps and most remote access. Admin accounts are only partially covered — assume privileged credential theft is viable.
Centralized logging Basis: CIS 8.2 (3/4), 8.9 (2/4), 8.10 (2/4), 8.11 (1/4)	Partial	Logging is enabled on key systems but centralization is incomplete and retention beyond ~30 days is not assured . Collect endpoint-local logs early; do not assume 90-day lookback.
Backups & recovery Basis: CIS 11.2 (3/4), 11.3 (3/4), 11.4 (2/4), 11.5 (1/4)	Partial	Automated, protected backups exist, but isolation from the domain is incomplete and restores were last tested over a year ago . Verify backup reachability before trusting recovery; assume ransomware may have touched them.

Network segmentation

Basis: CIS 12.2 (2/4), 12.8 (1/4); 3.3 (2/4)

Gap

Flat internal network beyond guest Wi-Fi separation. Assume lateral movement was unimpeded; scope broadly.

Security awareness / phishing readiness

Basis: CIS 14.1 (3/4), 14.2 (3/4)

In place

Active training program; users may self-report phishing — check the report mailbox for early indicators.

Vulnerability management

Basis: CIS 7.1 (2/4), 7.3 (2/4)

Partial

Patching is ad-hoc on servers. Internet-facing services may lag on patches — prioritize them in the initial-access hypothesis.

Coming soon: assertion-backed answers Placeholder

A future version of this brief will draw on directly-answered capability questions (e.g. "could ransomware reach your backups?") rather than deriving status from control scores. Statuses above are inferences from the framework assessment and are labeled with their basis.

First-hour suggestions for this environment

- **Contain identity first:** Entra ID is the control plane. Revoke sessions and reset credentials for affected accounts; remember admin MFA coverage is incomplete.
- **Preserve logs immediately:** retention beyond ~30 days is not assured. Export Entra sign-in logs, M365 audit, firewall, and endpoint logs before they age out.
- **Verify backups before you need them:** isolation is incomplete and restore testing is stale. Confirm at least one clean, reachable-but-not-domain-joined copy early.
- **Scope wide:** segmentation is a known gap; treat lateral movement as likely rather than possible.
- **Use what works:** EDR host isolation and the asset inventory are dependable levers here — lean on them for containment and scoping.

organization's key; distribute to responders at the organization's discretion.