Crusader Security

ILLUSTRATIVE SAMPLE

K-12 CYBERSECURITY ASSESSMENT

Security Posture Assessment

Northgate School District (fictional) · 240 staff · 3,100 students

Prepared by Crusader Security · Engagement window: 10 business days · Frameworks: CIS Controls IG1, NIST CSF

EXECUTIVE SUMMARY

Northgate's environment shows the profile we see across small districts: the fundamentals are mostly in place, but two **Critical** gaps — missing multi-factor authentication and an unprotected email domain — leave the district one phished password away from a serious incident, and would likely be flagged on a cyber-insurance renewal. None of the findings require new headcount or a large capital purchase. The roadmap on page 2 closes both Critical items in the first two weeks. This assessment reviewed identity, endpoints, email authentication, backups, and administrative access against CIS Controls IG1 and the NIST Cybersecurity Framework.

POSTURE AT A GLANCE

Overall security score

61/100

Moderate — meaningful gaps, none unfixable.

CIS IG1 controls met

34/56

22 controls need attention; 8 are quick wins.

Cyber-insurance readiness

At risk

MFA gap is a common denial trigger.

FINDINGS BY SEVERITY

2	2	2	0
Critical	High	Medium	Low

PRIORITY FINDINGS & RECOMMENDATIONS

CRITICAL **No multi-factor authentication on staff accounts**

Microsoft 365 sign-in logs show 214 of 240 staff accounts without MFA. This is the single most common cause of district account takeover and a frequent cyber-insurance denial reason.

→ **Enforce Conditional Access MFA for all staff; phased rollout with comms.**

CRITICAL **Domain accepts spoofed email (no DMARC)**

No DMARC policy is published. Attackers can send mail as @northgate.k12.us to parents and staff with no authentication check — the classic invoice-fraud and credential-phishing vector.

→ **Publish DMARC (p=none → quarantine → reject) with aggregate reporting.**

HIGH **Local admin rights on 1:1 student devices**

A sampled set of student Chromebooks and staff laptops grant standard users local administrator rights, letting malware install persistently.

→ **Remove local admin; deploy managed EDR with policy enforcement.**

HIGH **Backups are not tested or offsite-immutable**

Nightly backups run, but no restore test in 12 months and no immutable offsite copy — ransomware would encrypt primary and backup together.

→ **Add immutable offsite backups; quarterly restore tests.**

MEDIUM **Stale and over-privileged accounts**

18 accounts have not signed in for 90+ days, and 6 non-IT accounts hold Global Administrator. Each is an unused door left unlocked.

→ **Disable stale accounts; apply least-privilege to admin roles.**

MEDIUM **No written incident-response plan**

Staff have no documented steps or contacts for a security incident, adding hours of confusion during the event that matters most.

→ **Adopt a district IR plan; run a 2-hour leadership tabletop.**

90-DAY REMEDIATION ROADMAP

TIMELINE	WHAT WE DO	WHY IT MATTERS
Weeks 1–2	Enforce MFA on all staff accounts · publish DMARC/SPF/DKIM	Closes both Critical findings and the top insurance requirement.
Weeks 3–6	Deploy managed EDR · remove local admin · disable stale/over-privileged accounts	Removes persistence and lateral-movement paths.
Weeks 7–10	Immutable offsite backups + restore test · adopt IR plan + tabletop	Makes a ransomware event survivable and rehearsed.