Cybersecurity Posture Report

Combined — 18 Assessments

Executive Summary Report

CLIENT

District 101

Assessments Combined: 18

Total Findings: 203

Generated: 2026-06-30

COMBINED POSTURE SCORE

2.76 / 5.0

MEDIUM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

District 101 was assessed across 18 cybersecurity and IT-risk areas, producing 203 findings. Overall security posture scores 2.76 out of 5.0 — ahead of the national K-12 average of 2.54. 34 of those findings are critical, concentrated in Business Continuity & Disaster Recovery Policies, Facility Access Control, Mobile Device Management, and represent risk the district is carrying today without adequate protection in place.

This report summarizes those critical exposures, what they mean for the district, and the recommended path to close them. Full technical detail and the phased plan are provided in the accompanying Technical report and Remediation Roadmap.

Scope: 18 assessments combined, spanning governance, identity & access, data protection, detection & response, continuity, and third-party risk. Posture as of 2026-06-30.

AGGREGATE RISK POSTURE

34	79	90	0
CRITICAL	HIGH	MEDIUM	LOW

NIST CSF POSTURE

K12 SIX ESSENTIALS
2.80 / 5.0
Crosswalked from Discovery · no national benchmark

NIST CSF (OVERALL)
2.76 / 5.0
National K-12 average: 2.54 (NCSR)

The district has essential protections in place but applies them unevenly — the gaps that remain are the ones attackers actively look for.

The two scores measure the same posture against two yardsticks — the national cybersecurity standard (NIST CSF) and the K-12–specific essentials benchmark (K12 SIX).

BUSINESS IMPACT

District 101 carries 34 critical gaps that warrant near-term attention. They concentrate in Business Continuity & Disaster Recovery Policies, Facility Access Control, Mobile Device Management. Left unaddressed, these translate into concrete business risk:

- **Operational disruption** — A ransomware event or major outage could halt instruction, payroll, and core operations for days to weeks, with limited tested recovery capability.
- **Data exposure & privacy liability** — Gaps in access control and data handling raise the likelihood and severity of a student-data breach, carrying FERPA, COPPA, and state-law consequences.
- **Financial exposure** — Incident response, recovery, legal, and breach-notification costs — plus potential payroll or wire fraud — commonly reach six figures for a district-scale event.
- **Reputational & community trust** — Public disclosure of an incident affecting students erodes community confidence and draws board, media, and regulator scrutiny.

RISK APPETITE & EXPOSURE

Most K-12 districts hold a low tolerance for risks that interrupt instruction or expose student data, but limited budget and staff to act on that tolerance. The distance between that intended posture and the district's actual posture is its true exposure.

CURRENT POSTURE vs K-12 AVG
2.76 / 2.54 national avg

UNACCEPTED EXPOSURE
34 critical open now

Each critical gap is risk the district is carrying right now with no mitigating control in place. Closing the critical tier first is the fastest way to pull actual exposure back within the district's intended risk appetite; the phased Remediation Roadmap

sequences that work.

EXTERNAL THREAT LANDSCAPE

K-12 districts are among the most-targeted sectors in the United States. The gaps in this report should be read against the threats most active against schools today:

- **Ransomware** — Attackers encrypt district systems to halt instruction and operations, increasingly pairing encryption with theft and public-extortion of student and staff data.
- **Third-party & vendor compromise** — EdTech platforms and IT suppliers with access to district data are a leading breach vector; a single vendor incident can expose thousands of student records.
- **Phishing & credential theft** — Email attacks on staff remain the most common initial foothold, leading to account takeover, payroll and wire fraud, and lateral movement.
- **Student-data breach & extortion** — Student records — SIS, special-education, and health data — are targeted for theft and release-extortion, carrying direct FERPA and state-privacy exposure.

These are industry-wide patterns, not findings specific to this environment; they frame why the critical gaps below carry the weight they do.

TOP CRITICAL FINDINGS

The three most critical findings are shown below. The full set of critical, high, medium, and lower-severity findings is in the Technical report.

CRITICAL · EFFORT TO FIX: HIGH — IDENTITY & ACCESS MANAGEMENT DISCOVERY · ACCOUNT LIFECYCLE

Account Deprovisioning and Leaver Process

RISK & IMPACT

The lack of an automated account deprovisioning process poses a significant risk to District 101, as former employees may retain access to sensitive systems and data. This gap can lead to unauthorized access, data breaches, and compliance issues.

CRITICAL · EFFORT TO FIX: HIGH — MOBILE & ENDPOINT SECURITY DISCOVERY · MOBILE DEVICE MANAGEMENT

MDM Enrollment and Coverage

RISK & IMPACT

The lack of a comprehensive MDM enrollment process leaves devices unmanaged and vulnerable to security threats. This gap allows unauthorized access to company resources and data.

CRITICAL · EFFORT TO FIX: HIGH — MOBILE & ENDPOINT SECURITY DISCOVERY · MOBILE DEVICE MANAGEMENT

Mobile Application Management

RISK & IMPACT

The absence of a mobile application management policy enables unregulated app installations, introducing potential security risks and data breaches.

+ 31 additional critical findings — see the Technical report for the complete list.

RECOMMENDED NEXT STEPS

To bring exposure back within the district's risk tolerance, we recommend:

- **Approve the phased Remediation Roadmap** — and fund Phase 1 (Foundations), which targets the 34 critical gaps over the first 0–6 months.
- **Assign an accountable owner** — for the security program, with a regular cadence for reporting progress to leadership and the board.

- **Close the critical tier first** — before lower-severity work — these gaps carry the greatest likelihood and impact.
- **Re-assess after Phase 1** — to confirm the critical exposure has been closed and to measure improvement against this baseline.