



Scottsdale *Unified*
SCHOOL DISTRICT



IT Vision and Mission

Our vision is to **support a dynamic, technology-rich environment** that empowers all students and staff to become passionate life-long learners and productive participants in our society.

Our mission in integrating technology is to enable staff and students to be **academically successful, technologically aware and fully engaged in the learning process.**



K-12 Cybersecurity Threat Statistics

[2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience](#)

*This report is the backbone of our vision for the future Empowering the Human Element and a Culture of Cyber Empowerment

- **82% of U.S. K-12 schools experienced a cyber incident** between July 2023 and December 2024.
- In that same study, **over 9,300 confirmed incidents** occurred across about **5,000 school systems**.
- School districts experience **about 5 cyber incidents per week on average** nationwide.
- More than **1,600 publicly disclosed cyberattacks** targeted schools between 2016–2022.



National Institute of Standards and Technology (NIST) Cybersecurity Framework

- **Govern:** Establish policies, define roles and responsibilities, and promote cybersecurity awareness across the organization.
- **Identify:** Asset management, risk management strategy development, and identifying critical functions that, if disrupted, would impact the organization.
- **Protect:** Implement safeguards like access controls (e.g., multi-factor authentication), data security (encryption, backups), awareness and training, and protective technology (firewalls, antivirus).
- **Detect:** Continually monitor, implement threat detection technologies, and conduct security event analysis to find and investigate unusual activities.
- **Respond:** Incident response planning, containment and mitigation of breaches, communication strategies, and legal considerations.
- **Recover:** Developing and practicing recovery plans, ensuring backup and disaster recovery capabilities, learning from incidents, and communicating recovery progress to stakeholders.



Cyber Security Insurance Requirements

The Trust

- Secure Air-Gapped Backups – Barrier between our network and our back-ups
- Phishing Simulations and Training – Raise awareness around the need to be aware
- Multi-Factor Authentication (MFA) – App on our phones and tokens for folks without cell phones
- Vulnerability Scanning – Penetration testing
- Endpoint Detection and Response (EDR) Software -
- Software Patching – Regular Maintenance Schedules
- Managing End-of-Life Software – Windows, Mitel



Executive Summary: 2025-26 Trust Audit

The district demonstrated a strong and well-managed cybersecurity program, earning an overall risk assessment score of 96. Their technology team maintains a mature security posture supported by proactive governance, modern security tools, and consistent operational practices. The district successfully meets all **Trust Cyber Requirements**, including **multi-factor authentication (MFA)**, **endpoint detection and response (EDR)**, **phishing simulations and training**, **external vulnerability scanning**, **air-gapped backups**, **end-of-life software management**, and **structured software patching processes**. These safeguards significantly reduce exposure to ransomware, credential compromise, and other common cyber threats.

A small number of enhancement opportunities were identified. Full encryption of endpoint and server hard drives has yet to be implemented, and administrative personnel currently use standard accounts with elevated privileges rather than separate dedicated administrative accounts. Addressing these items will further strengthen protection against unauthorized access and data exposure. Overall, the district maintains a highly resilient cybersecurity environment and is well positioned to continue advancing its security maturity.



Summary of Results

- Overall Security Score
 - 96%
- Letter Grade
 - B (capped at B)

RISK LEVEL	COUNT
High Risk	0
Moderate Risk	2
Low Risk	67

90-100% Excellent - Strong cybersecurity posture



Section Scores

NO. SECTION SCORE

1.0 Inventory and Control of Assets **100%**

2.0 Account Management **100%**

3.0 Data Protection **63%**

4.0 Secure Configuration of Enterprise Assets **97%**

5.0 Malware Defense **100%**

6.0 Data Recovery **100%**

7.0 Security Awareness **100%**

8.0 Vendor Management **100%**

9.0 Incident Response **95%**

11.0 Financial Exposure **100%**



Key Findings

3.2 **COMP** Do administrators have separate dedicated admin accounts for conducting high-privilege tasks?

Status: **NOT IMPLEMENTED**

Points: 0/2.5 pts

Risk: **MODERATE**

Comments:

Administrative accounts currently use standard credentials with elevated privileges; plan underway to implement separate privileged admin accounts.



Key Findings

Moderate Risk Findings (1)

TIER 1B - Foundational controls require scheduling remediation activities.

3.3 **1B** Does the district encrypt hard drives on endpoints, servers, and on-premises backups?

Category: Data Protection

Status: **PARTIALLY IMPLEMENTED**

On prem backups are encrypted.



Google Audit – 180 pages – Four Hour Review

We earned a 9 out of 10.

Hard pressed to find a “real” issue 😊

Each item flagged was something that Google documents as the correct course of action somewhere else.

In other words, they understand the decision in one environment over another but still flag it for purposes of ongoing consideration

For example...

Google suggests we turn off: Google Sites, Profile Editing, Offline Access (docs, calendars...), Google Take Out, Google Notes

Once audit complete – take to Cabinet to review what is enabled or not



Ongoing Efforts & Measurables

Tabletop Exercises

Debriefs after incidents

Finance Audit

Trust Audit

Penetration Audit

Cyber Security Awareness – MSIC – use EDL lists



Ongoing Projects

Active Directory (AD) Clean-Up

Mitel to Ring Central

Jamf

Windows 11

Server upgrades

Erate – Mohave Network Refresh

Warehouse, Building Services Network Refresh

NOC

Upgrading Internet and Bandwidth at sites with network upgrades – more to come with a potential bond



Questions?