Cybersecurity Readiness Report for Valier School District
Date: July 18, 2025

---

1. Overview

This report evaluates the cybersecurity posture of Valier School District based on technical scans (DNS, DMARC, and port scanning) and a self-reported security questionnaire. The findings reflect a strong commitment to foundational cybersecurity practices across user access, email protection, network exposure, and staff awareness.

---

2. Organizational Information

- **Organization Name:** Valier School District
- **Email Domain:** valier.k12.mt.us
- **Website Domain:** www.valier.k12.mt.us
- **External IP (Firewall):** 216.220.16.170
- **Website Hosting IPs:** 216.239.32.21, 216.239.34.21, 216.239.36.21, 216.239.38.21
- **DNS Hosting:** Managed by University of Montana (umt.edu nameservers)

---

3. Security Questionnaire Review

Security Control	Status
MFA for Email	✅ Yes
MFA for Computer Login	✅ Yes
MFA for Sensitive Systems	✅ Yes
Acceptable Use Policy	✅ Yes
New Employee Security Awareness Training	✅ Yes
Annual All-Employee Security Training	✅ Yes

Summary: The district reports complete implementation of basic cyber hygiene practices, especially

user authentication (Multi-Factor Authentication) and routine training. This indicates a proactive and policy-driven approach to risk mitigation.

---

4. DNS & Email Security

DNS Records

- DNS is managed by the University of Montana (cudess1.umt.edu, cudess2.umt.edu), suggesting centralized and professionally administered DNS.
- A records point to IPs within Google's network (likely Google Sites hosting for web content).

MX Records (Email)

- The district uses Google Workspace (Gmail) for email, as shown by multiple aspmx.l.google.com MX records.
- SPF record is correctly configured:
  v=spf1 include:_spf.google.com include:mg.infinitecampus.org -all
  This helps mitigate spoofing by defining authorized mail senders.

DMARC Record

- A valid DMARC record exists with a **reject** policy:
  v=DMARC1; p=reject; rua=mailto:dmarc@valier.k12.mt.us
  This instructs receiving servers to reject unauthenticated mail, providing strong protection against phishing.

Conclusion: DNS and email protections (SPF, DMARC, and hosting security) are configured correctly and follow best practices.

5. Port Scanning Results

Website Hosting (Google IP: 216.239.32.21)

- **Port 80 (HTTP):** Open
- **Port 443 (HTTPS):** Open
  These are expected for a publicly accessible website and are typical for Google-hosted services.

Firewall / External IP (216.220.16.170)

- **All scanned ports are closed**
  This is a strong sign of network perimeter hardening and good firewall configuration. No externally exposed services were found on the organization's primary IP.

---

6. Risk Assessment & Readiness Summary

Category	Status	Notes
Authentication Security	✅ Strong	MFA is required across key systems
Email Security	✅ Strong	SPF and DMARC with "reject" policy in place
Network Exposure	✅ Secure	No exposed services on the external firewall IP
Web Hosting	✅ Secure	Google-hosted; limited attack surface
Policy & Training	✅ Comprehensive	Acceptable use policies and regular training in place

---

7. Recommendations

Although the cybersecurity readiness is solid, continuous improvement is essential. We recommend the following:

1. **Verify DKIM**: While SPF and DMARC are configured, ensure **DKIM** is also active for all sending domains.
2. **Vulnerability Scanning**: Consider regular internal and external vulnerability assessments of network devices and servers.
3. **Incident Response Plan**: Document and regularly test a cybersecurity incident response and disaster recovery plan.
4. **Asset Inventory**: Maintain a regularly updated inventory of hardware/software assets and monitor for unauthorized changes.
5. **Third-party Risk**: Evaluate vendors (e.g., Infinite Campus) for their security posture, especially since they're included in SPF.

---

8. Conclusion

Valier School District demonstrates a strong cybersecurity foundation, particularly in authentication, email protection, staff training, and perimeter security. Continued vigilance and regular audits will help maintain and improve this strong security posture.

Prepared by:
Cybersecurity Assessment Team
Date: July 18, 2025