Cybersecurity and Trust Coverage

Cyber threats are no longer rare or isolated—they're a daily reality for school districts. In response, the Trust has put in place practical measures to reduce risk and give members greater confidence in their digital security.

Trust Cyber Requirements

At the core of our efforts are seven cybersecurity controls each district must adopt to establish eligibility for full cyber liability coverage:

1. **Air Gap Backups:** An air gap backup system, tested and validated for recovery capability at least twice each year.
2. **Phishing Simulations and Training:** Quarterly events—phishing simulations, awareness training, or a combination.
3. **Multi-Factor Authentication (MFA):** Multi-factor authentication for all employees and all remote access connections.
4. **External Vulnerability Scanning:** A quarterly, non-intrusive network scan identifying and reporting security weaknesses (vulnerabilities) on an organization's publicly exposed network assets, such as firewalls, web or email servers, and IoT devices.
5. **Endpoint Protection:** Endpoint detection and response (EDR) software for real-time threat detection and response on end-user devices. (The free Windows Defender program is not considered EDR for purposes of this Trust requirement.)
6. **Software Patching:** Installation of critical and high-severity patches within 7 days, and all other software patches within 30 days.
7. **End-of-Life Software Protection:** Implementation of measures to protect and segregate end-of-life software and systems.

These controls are essential for reducing vulnerabilities, enhancing cyber resilience, and aligning with industry best practices.

Cyber Liability Coverage Options

The Trust offers four distinct cyber liability coverage options, each tailored to reflect a district's compliance with the required cybersecurity controls.

The table below provides an overview of these options:

Coverage Program	District Compliant with Trust Cyber Conditions?	District Pays Cyber Coverage Contribution?	Limits and Deductibles Offered
Limited	No	Yes	$250,000 per occurrence; $100,000 deductible
Basic	Yes	Yes	$1,000,000 per occurrence; $5,000 deductible
Enhanced	Yes	Yes	$3,000,000 or $5,000,000 per occurrence; $5,000 deductible
Opted out	No	No	None

The seven cybersecurity controls are required for Basic or Enhanced Cyber Coverage. This aligns with market expectations and is critical for mitigating cyber risks in today's environment.

Districts that have not adopted the controls qualify only for Limited Cyber Coverage. To further incentivize adoption, the deductible for the Limited Coverage Program was increased to $100,000 beginning July 1, 2025, while maintaining the existing coverage limit of $250,000.

Why the Controls Matter

The Trust's cybersecurity requirements are designed to protect member districts from the growing threat of cyberattacks. We encourage all districts to prioritize adoption of these controls, not only to qualify for higher levels of coverage with lower deductibles, but to reduce their exposure to cyber risks.

For additional information or assistance with meeting the cybersecurity requirements, please contact our cyber team at cyber@cyberpools.org.