Renewal 2025

CSDSIP Colorado School Districts Self Insurance Pool

Tips & Tricks: 2025 Cyber Application

CSDSIP currently offers our Members the opportunity to add Cyber coverage to complement our core policy. Our Cyber coverage is a supplementary coverage and is issued as stand-alone insurance policy with its own Declarations Page, Conditions, Insuring Agreements, and Endorsements.

Compliant Members vs Non-Compliant Members

- Members who answer "Yes" to all 6 of the Minimum Control Requirements on our 2025 Cyber Application will be deemed a "Compliant Member" by our Cyber carrier. Compliant Members are eligible for $1 million Cyber limits with a deductible of $25,000 for Members with fewer than 9,000 students and $50,000 for Members with more than 9,000 students.
- Non-Compliant Members will be offered $250,000 in Cyber limits with a deductible of $50,000 for Members with fewer than 9,000 students and $100,000 for Members with more than 9,000 students.

Why Become Complaint Now?

We cannot change your compliancy status midterm. As such, we strongly recommend that if you are not currently Complaint that you take the time now to become Compliant before June 30, 2025.

Not Currently Complaint?

CSDSIP has partnered with Gallagher Cyber Defense Center ("Gallagher Cyber") with the goal of working with all of our Members to be Compliant. They offer a collection of tools and services to assist our Members with taking a proactive and continuous approach to managing their cyber risk. This includes access to cyber risk specialists and security technology to help our Members avoid cyber breaches.

Their team are available to help you meet our Minimum Control Requirements that you need assistance with. You can contact reach them at CyberRMcdc@ajg.com or Reis_Brooke@ajg.com (keeping in mind they are 7 hours ahead of us).

Cyber Tips & Tricks

Below please find the Minimum Control Requirements questions on the Cyber Application (starting at question #3) along with a summary of the services available to you to assist you with becoming Compliant.

Members who have Cyber coverage through CSDSIP, have access to the Cyber Defense Center, a platform that includes several tools and service including vulnerability scanning, threat intelligence webinars, secure humans, Gallagher cyber-risk matters newsletter, and Virtual Chief Information Security Officer (CISO) access. Click here for the link to Gallagher Cyber's Defense Center Access Instructions.

Virtual Chief Information Security Officer (CISO)

Gain access to Gallagher Cyber's Virtual Chief Information Security Officer (CISO), who will provide guidance and support throughout your service. Leverage their expertise to assess your current cybersecurity posture, develop strategies, and address any concerns or questions you may have.

This service can help you answer the following questions:

#3 – Do you have Multi-Factor Authentication (MFA) for all remote systems access and domain admin access?

#4 – Do you have a credible Endpoint Detection Response (EDR) tool in place and active?

#5 – Are data backups either:

a. Stored offline and require credentials separate from your active directory to access; or

b. Stored in a cloud service designed to protect data from a ransomware attack?

#7 – Are firewalls and antivirus software in place, and updated with critical patches within 30 days of release?

Security Awareness Training

The biggest contributor to cyber incidents is human vulnerability. Each quarter, Gallagher Cyber hosts a series of cybersecurity training webinars designed for your employees at all levels of understanding. Throughout the year, your staff can be trained by their specialist cybersecurity team in the role they can play in defending your organization. Topics will include boundary control, email security and phishing, working from home, data protection, and more.

In addition, CSDSIP Members have access to our Vector Solutions Training Platform which offers the following Cybersecurity Awareness Training for employees:

- Classifying and Safeguarding Data for Organizational and Personal Use
- End-User Best Practices
- Security Awareness Essentials
- Social Engineering

Any class would meet this requirement. You can reach out to our Risk Control Team to get set up on the Vector Solutions Training Platform if you have not already.

These training opportunities can help you answer "Yes" to the following question:

#6 – Have your employees completed cyber security awareness training in the last 12 months?

Clarification Item – In prior years, this question asked if certain groups had taken this training. The carrier is looking for meaningful attempts by our Membership to train as much of their staff as practical. Keeping in mind that it takes one person to open a link in a phishing email to allow a virus to come into your system, we strongly recommend (though not required by this question) that all your staff annually take cyber security awareness training.

Network Vulnerability Scans

Gallagher Cyber will monitor your external boundaries and provide you with updates every day as to the known vulnerabilities in your technology portfolio. This report will outline where your low-, medium-, and high-risk technology vulnerabilities reside.

This scan can help you answer "Yes" to the following question:

#8 – Are network vulnerability scans done regularly?

Clarification Item – Members who have our Cyber coverage can answer "Yes" to this question. However, to ensure that you are Compliant, you also need to pull these reports on a regular basis and take action on what was found.