CSD Pool Cybersecurity Review and Discussion, Feb. 21, 2024

As a CSD Pool member that has qualified for a higher sublimit upon completion of a NetDiligence Quiet Audit cyber assessment or eligible third party assessment, you will need to demonstrate next steps taken in order to keep those limits through 2025. This applies to members that have already completed a cyber assessment prior to September 30, 2023.

The next steps are easy, and they can be completed at any meeting of the Board of Directions held by your district throughout the year. To maintain the higher $1,000,000 sublimit, we simply require a copy of the meeting minutes in which the following has been discussed:

1. **The district's current exposure to Personally Identifiable Information (PII)**
2. **Progress made to any recommendations or findings identified in the initial NetDiligence Quiet Audit cyber assessment**
3. **Next steps to be taken over the next twelve (12) months regarding the district's cybersecurity**

To keep the higher $1,000,000 sublimit in place, we must receive a copy of the applicable meeting minutes by September 30, 2024. Any meeting minutes will suffice as long as they discuss the criteria outlined above and took place between October 1, 2023 and September 30, 2024.

Safeguarding Personally Identifiable Information (PII)

Multiple data protection laws have been adopted by various countries to create guidelines for companies that gather, store, and share the personal information of clients. Some of the basic principles outlined by these laws state that some sensitive information should not be collected unless for extreme situations.12

Also, regulatory guidelines stipulate that data should be deleted if no longer needed for its stated purpose, and personal information should not be shared with sources that cannot guarantee its protection.1

Cybercriminals breach data systems to access PII and then sell it to willing buyers in underground digital marketplaces. For example, in 2015, the IRS suffered a data breach leading to the theft of more than a hundred thousand taxpayers' PII.3

Steps taken:

Replacement of LastPass with Bitwarden password manager. All library staff are being trained in using this product.

Reviewing 2-step authentication; we're currently working with security keys and authenticators experimentally.

Twelve-step plan

Continued removal of users no longer active in the library system.

Continued removal of non-essential user information: birthdates, gender, considering contact information such as email addresses and residence addresses.

In-library privacy practices.

Annual review of staff and user policies.

Continued staff training

Breach planning – local practice as well as consideration of commercial products (e.g. breechplanconnect.com).

Continue to involve the board of trustees in cyber policy planning

Installation of interior and exterior security cameras.

Password protection for all staff and board members holding library passwords.

Review and harden the library webpage.