# STUDENT DATA Loss Prevention

## BLOCKING

Many district data systems are behind network firewalls and not publicly accessible from the internet. The district is implementing Network Intrusion Prevention systems to detect and block attempts to breach network security and additional controls to protect URLs from external attacks.

## SHARING

Student data that is shared with 3rd party curriculum vendors is done on an as needed basis under a written NDA agreement between each vendor and the district. Student data that is transferred to 3rd party vendors is secured and encrypted manner. The majority of student data shared is brokered through a 3rd party iKeepSafe certified partner.

## PHISHING

The district has a sophisticated e-mail firewall and filtering technology that identifies and blocks the majority of phishing attempts. The district is implementing periodic simulated phishing campaigns to obtain data on which employees are susceptible to phishing, as well as security awareness training courses to raise awareness around phishing, social engineering, and safe internet practices.

## MONITORING

The district is implementing software to monitor and alert security administrators if sensitive data leaves the district in an insecure manner or if it appears in employees' cloud storage accounts.

## HARDENING

The district has relocated, upgraded, and hardened the data center to increase resilience to a disruption in service.

## INSURING

The district has increased cybersecurity insurance policy in addition to taking steps to prevent device loss such as permanent device lid etching.