Greg Martin, Director of Technology
Administration Service Center
28W250 St. Charles Road
West Chicago, IL 6018
(630) 876-7800
www.benjamin25.org

Benjamin
SCHOOL DISTRICT 25

TO: Board of Education
Dr. McGill
FROM: Greg Martin, Director of Technology
DATE: December 2, 2025
RE: Technology Report

Dear Board of Education Members,

The list below highlights a few of the updates and accomplishments over the past month:

- **EVO Configuration:**
  We have completed the configuration of EVO multi-factor authentication (MFA) for both Active Directory and Google Workspace, and we have begun the testing phase to ensure a smooth transition from our legacy SassPass platform. EVO MFA provides stronger security, improved reliability, and better integration with our systems, supporting the district's cybersecurity goals. Once testing is completed, we will begin migrating staff from SassPass to EVO in a phased approach to minimize disruption and ensure a seamless user experience.
- **Additional YouTube Student Filtering:**
  Enhanced our existing Securly web-filtering system by adding an additional layer of protection through the Securly Chrome extension. This extension provides more granular YouTube controls, allowing us to block comments, hide suggested videos, and strengthen content filtering for students.
- **Server Patching and Maintenance:**
  Completed server patching and maintenance across all district servers to ensure optimal performance, stability, and security. This maintenance included applying operating system updates and firmware patches, helping protect district systems against emerging vulnerabilities.
- **Updated Firewall Firmware:**
  Updated the district's firewall to the latest firmware version, ensuring improved security, enhanced performance, and continued reliability of our network infrastructure. This update provides essential vulnerability patches and feature improvements to help maintain a secure and stable environment.
- **December 2025 Secure Halo Newsletter Summary on Internet-Of-Things (Iot):**
  A recent EdScoop report highlights an alarming 860% surge in cyberattacks targeting IoT devices across the education sector, underscoring the growing risk posed by connected classroom and building technologies (EdScoop Staff, 2025). These attacks often exploit outdated firmware, weak segmentation, and limited visibility into connected systems. In response to these emerging threats, our district maintains a complete inventory of all IoT devices, conducts monthly network vulnerability scans, monitors for and is alerted to unusual or suspicious network traffic, and routinely patches devices with the most current firmware. These practices strengthen our overall cybersecurity posture and align with SOPPA's requirements for reasonable and proactive security measures.