Eisenhower Cooperative

a case study

EISENHOWER Cooperative

Investing in technology to better support students and teachers

The mission of the Eisenhower Cooperative is to provide specialized services and enhance educational opportunities for all students in the member districts. This will be accomplished by the committed effort of the districts working collaboratively and efficiently.

The Eisenhower Cooperative believes

- Every child can learn
- Every child is a valuable resource
- In meeting the needs of all children
- All students must be treated with dignity and respect
- In developing independent and life-long learners
- In fostering the acceptance of diversity
- In a safe, secure, supportive learning environment
- In collaborative teamwork including all students, families, staff, community, and agencies
- In responsibly utilizing all resources within and outside the organization
- All students should have access to a curriculum aligned to state standards
- In fostering students' self-esteem

Main Challenges

Hardware

The Eisenhower Cooperative had 5 physical servers, each server already passed it's end of life and was at risk of going offline. Three of those servers were running an operating system that was at end of life, thus would no longer be supported by the manufacturer.

Backup and Disaster Recovery

The Backup and Disaster Recovery strategy was relying on an old tape backup system and manually taking the backup tapes home every day for offsite redundancy. No data verification was happening to ensure the data was intact and would be able to restore from.

- In a best-case scenario, the time to recover from a disaster using this backup strategy was 2-4 days.

Logistics

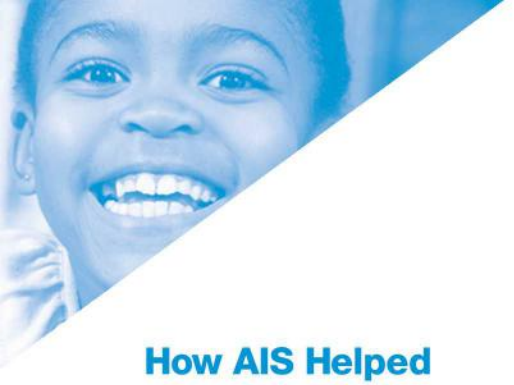
Eisenhower Cooperative has classrooms located in several districts with no way to authenticate or apply policies to.

- There were security concerns with teachers and students not authenticating to access network resources like files and printers.
- In addition, many teachers were experiencing problems printing and accessing the internet.

Desktop and Laptop Security

There was no way to manage updates on the Operating Systems and 3rd party applications like Adobe on the desktops and laptops at Eisenhower's remote classrooms. Desktops were collected at the end of the year to deploy patches and updates.

- This created many security vulnerabilities within those remote environments.



How AIS Helped

Hardware Challenges

Rather than purchasing multiple physical servers to replace the aging hardware, AIS leveraged virtualization via VMware to run multiple servers on one piece of hardware (called a 'host'). AIS consolidated the 5 servers down to 2 and migrated the data into the latest Microsoft server operating system.

- This saved Eisenhower Cooperative thousands of dollars in hardware and licensing costs.
- The new VMware host was also configured to allow for future growth.
- By having a host with extra capacity, their physical phone server was easily migrated to the host when the phone server's hardware became end of life.

Backup and Disaster Recovery Challenges

AIS installed a fully managed Backup and Disaster Recover appliance, known as a BDR, to handle their backup and disaster recovery strategy moving forward.

- The added ability to turn backups into virtual machines on the local appliance transformed the time to recover from a disaster from days to hours.
- By automatically replicating backup data to a secure cloud, backups no longer need to be brought home.
- Backups are now verified by our Network Operations Center (NOC) in real-time to ensure data integrity.
- The cloud replicated data can also be used to create a Disaster Recovery Site within hours providing a true end-to-end Disaster Recovery Solution.

Logistical Challenges

AIS implemented a secure wireless network for Eisenhower's remote classrooms that connected back to the main location by a site-to-site VPN tunnel. Following AIS and industry best practices, a server was installed in the building where the remote classrooms were located. Ensuring login times for teachers and students would remain optimal.

- Security policies were applied to these remote classrooms mitigating security concerns.
- A policy was created to ensure teachers at remote locations were connected to the printer they needed to print to eliminating printing issues.
- Our network monitoring identified the root cause of internet problems and were remediated.

Desktops and Laptops were not secure throughout the year

By utilizing AIS's managed service platform, desktops and laptops are kept up to date throughout the year.

- A testing and whitelisting process ensures patches and security updates don't create additional issues.
- 3rd party applications like Java, Adobe and Chrome are kept up to date as well.

What's Next for Eisenhower Cooperative?

Eisenhower Cooperative continues to invest in technology to support their students and teachers. As Eisenhower Cooperative expands its reach, so does AIS's. Our next projects will be connecting additional remote classrooms to the Eisenhower network and implementing Google Classrooms. Both initiatives will ensure teachers and students are secure and operating efficiently.