Morton IT Department
December 2025 Update

1. Firewall Upgrade

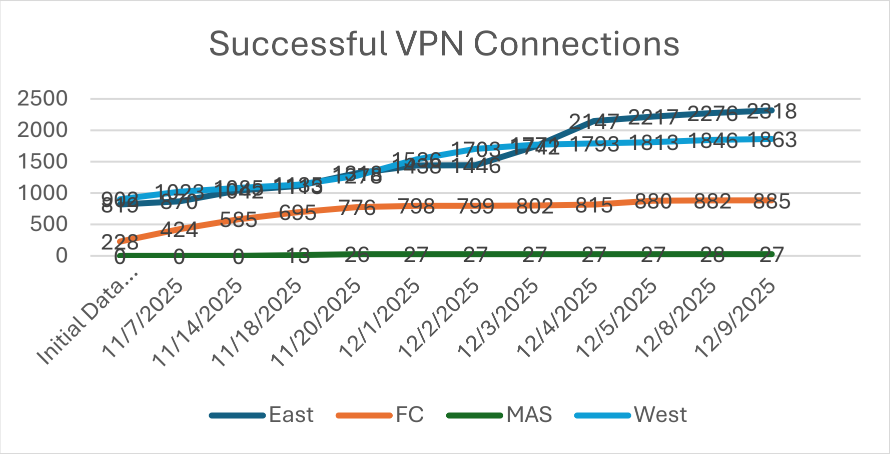
- The Morton IT Department continues to strengthen the district's cybersecurity posture by implementing the latest Cisco firewall hardware and software. These upgrades modernize our network infrastructure, increase reliability, and ensure alignment with current security best practices across education and enterprise sectors. The anticipated project completion date is **June 15, 2026**.
    - **Phase One - Completed September 2025**
        - This initial phase established the foundation for all subsequent upgrade work. The district's firewall software was elevated to a newer, more stable version, resolving several ongoing challenges related to web filtering and VPN connectivity. This upgrade improved reliability, enhanced compatibility with modern tools, and created a more flexible environment for future security enhancements.
    - **Phase Two – Began October 2025 (In Progress)**
        - **Firewall Hardware Procurement and Configuration**
            - During this phase, quotes for the new Cisco firewall hardware were secured, and the Board of Education approved the proposal at the November 2025 meeting. The hardware has been ordered and is scheduled to arrive in late December.
            - Configuration work is now underway in partnership with Sentinel, Morton's managed service provider. Sentinel has served as a strategic partner throughout the Firewall Upgrade Project and continues to lead the configuration and planning efforts. This preparation ensures a seamless transition to the upgraded firewall environment planned for the next phase.
        - **Firewall Dashboard Upgrade for Remote-Access Visibility**
            - A major advancement in this phase was the upgrade to the firewall monitoring dashboard. This enhancement now allows

the district to accurately identify which students have and have not successfully connected remotely to Morton’s infrastructure—whether from home or off-campus locations. This improved visibility has been instrumental in guiding student support, troubleshooting, and instructional planning.

- **VPN Engagement Blitz (IT, Data Team, and Building Administration Collaboration)**
    - Using the new dashboard data, the IT Department, Data Team, and building administration jointly initiated a districtwide VPN Engagement Blitz. This initiative ensured students received targeted training and support to connect successfully from home. Building administration developed structured plans informed by the dashboard insights, enabling schools to identify students needing additional assistance and to coordinate the necessary support to ensure full remote-access readiness.
    - The VPN Engagement Blitz continues on a smaller, ongoing basis at each campus. Building administration is now bringing students individually or in small groups to the Technology Service Internship (TSI) program, where TSI students provide one-on-one assistance in connecting to the VPN. This scaled-down model minimizes instructional disruption—especially as the semester concludes—while maintaining the district’s commitment to ensuring that all students have reliable access to learning materials from home.
    - The data on the next page indicates where each campus began at the start of the initiative and where they currently stand in terms of successful remote VPN connections.

Students Who Have Successfully Connected Remotely Utilizing Morton's Upgraded Firewall/VPN

	East	FC	MAS	West
Initial Data	819	228	0	902
11/7/2025	870	424	0	1023
11/14/2025	1042	585	0	1085
11/18/2025	1113	695	13	1135
11/20/2025	1318	776	26	1278
12/1/2025	1438	798	27	1536
12/2/2025	1446	799	27	1703
12/3/2025	1742	802	27	1771
12/4/2025	2147	815	27	1793
12/5/2025	2217	880	27	1813
12/8/2025	2276	882	28	1846
12/9/2025	2318	885	27	1863



	Total Enrollment	% of Student Population Connected 12/9/2025
East	3019	77%
FC	928	95%
MAS	44	66%
West	3202	58%
	7193	71%

- **Phase One – Planned for Spring Break 2026**
  - This phase will complete the initiative with a full hardware replacement using the newest Cisco appliance models.

Both Phase One and Phase Two are essential prerequisites that prepare the environment and configurations for this final hardware leap.

Once complete, the upgraded firewall ecosystem will deliver advanced intrusion prevention (Snort3), application visibility, real-time traffic analytics, and centralized management across the district.

All core network services, including SIS, email, and cloud integrations remained stable during and after Phase One implementation.

The project continues in partnership with Sentinel Technology and Cisco, coordinated within scheduled maintenance windows to minimize classroom and office impact.

---

2. Internet Service Provider Switchover Project Update

- Morton has partnered with AT&T as its Internet service provider for the past several decades. Through the federal E-Rate procurement process, a new multi-year contract was awarded to the Illinois Century Network (ICN). As part of this transition, each campus will move from a 2 Mbps connection under AT&T to a significantly increased 10 Mbps connection provided by ICN. Planning and preparation for this transition began in August 2025.
  - Phase One - East Campus Switchover Completed November 14, 2025
    The first campus to migrate to ICN was Morton East. The work involved three major stages:
    - Community Fiber Installation and Campus Termination
      ICN initiated the project by installing new fiber throughout the surrounding community and terminating the connection at the East campus. This step required substantial coordination and was completed successfully prior to the switchover.
    - Firewall Port Configuration and Infrastructure Alignment
      Once the fiber work was complete, Morton’s IT team coordinated efforts between Sentinel (our managed service provider) and ICN to ensure the district’s firewall environment could support the increased bandwidth. This included upgrading firewall firmware and configuring all necessary ports to accept the new data flow.

        - External Vendor Coordination and Security Assurance
          The district worked closely with its external partners—including Skyward, Ivanti, RingCentral, and TrueTime—to ensure all services were prepared for the updated IP addresses. At the same time, the IT Department maintained security requirements across multiple VPN tunnels and vendor integrations.
        - To minimize instructional disruption, the actual switchover occurred on Friday afternoon, November 14, after students and staff had left for the weekend.
        - As with any ISP transition of this complexity, there were coordination challenges involving several outside vendors. A few systems required follow-up adjustments the following week—such as library databases, timeclocks, and helpdesk portals—but the extensive planning and preparation significantly reduced the impact on teaching and learning.
        - Following the transition, an After-Action Review was conducted to evaluate the process and refine procedures for future cutovers. Adjustments have been made, and the next migration.
    - **Phase Two - Morton West Switchover**
        - West is scheduled for **December 19**, 2025 coinciding with the start of Winter Break to again minimize the impact on instruction.

---

3. SailPoint Identity & Access Management (IAM) Project Update

SailPoint, Morton's new Identity and Access Management (IAM) platform, was approved by the Board of Education in May 2025. The district partnered with KeyData to serve as Morton's Managed Service Provider (MSP) for the first three years of implementation. This project positions Morton to modernize account provisioning, strengthen cybersecurity, and streamline identity processes across all systems. The initiative is structured into three primary phases:

- **Phase One — System Connections and Data Source Integration**
    - The first phase focused on establishing the foundational connections between SailPoint and Morton's core identity systems. This included:
        - Designating Skyward Finance and Skyward Academic as the authoritative sources of employee and student data.
        - Connecting SailPoint to Azure Active Directory and Office 365 to automate account creation and assign licensing based on job roles.
        - Creating an integration with RingCentral to automatically provision phone numbers aligned to employee job titles.

- **Phase Two – Testing, Cleanup, and Portal Preparation (To Be Completed Before Winter Break)**
    - With the technical connections in place, the second phase shifted to testing within a dedicated "Sandlot environment." This step allowed the district and KeyData to evaluate the new provisioning workflows and identify necessary adjustments before going live. Key tasks included:
        - Removing inactive accounts from Azure and Skyward to eliminate legacy data conflicts.
        - Documenting and refining HR workflows to ensure consistency and accuracy in employee onboarding.
        - Reviewing manual IT processes so SailPoint can fully automate them moving forward.
    - Phase Two is scheduled to be completed before Winter Break, and the SailPoint portal will go live in January 2026, managed operationally by KeyData.
- **Phase Three – Monitoring, Optimization, and Expansion (Wi**
    - The third phase will focus on ongoing monitoring and fine-tuning of the IAM environment to ensure stability, accuracy, and security. During this phase, the district will also expand SailPoint's integrations to include additional systems, such as:
        - DUO, Morton's multifactor authentication (MFA) solution
        - KanTech, Morton's electronic keycard access system
    - These expansions will extend SailPoint's automation capabilities and further unify security and access control across the district.

4. Uninterruptible Power Supply (UPS) Infrastructure Project Update

Uninterruptible Power Supplies (UPS) have historically been installed at each campus's Main Distribution Frame (MDF) to protect core network systems. Two years ago, the district expanded this strategy by purchasing UPS units for all Intermediate Distribution Frames (IDFs)—the locations that house switches and critical network equipment throughout the buildings. Installing UPS units at both the MDF and IDF levels protects Morton's infrastructure from electrical surges, maintains network uptime during short power interruptions, and enables controlled shutdowns during extended outages to prevent data loss.

Although the UPS units were purchased, they were not installed or configured due to the network intrusion incident that halted all district technology projects. This fall, the IT Department reprioritized and relaunched the initiative, bringing the project **to** approximately 95% completion**.**

- **Phase One – Inventory and Status Verification**
  - The first phase involved identifying every IDF closet and assessing the status of the UPS units assigned to them. While most units were physically present, many were not connected to power or integrated into Morton's network. The IT team, in partnership with BlueWire, reviewed and corrected the setup in all 43 IDF closets, ensuring each UPS was properly powered and connected.
- **Phase Two – Network Card Installation and Centralized Monitoring**
  - During the second phase, network interface cards were installed in each UPS and connected to the district's data network. This allowed all UPS units to be monitored through a single, centralized dashboard. Central monitoring enables real-time alerts, streamlined maintenance, and proactive identification of power-related vulnerabilities.
- **Phase Three – Ongoing Monitoring, Firmware Updates, and Mitigation**
  - Phase Three, which continues today, focuses on continuous monitoring and applying firmware updates across all connected UPS devices. This effort has already identified potential weaknesses that the IT team is actively addressing. Importantly, the strengthened UPS infrastructure has already prevented two campuses from losing network communication during recent localized power outages.
- **Next Steps**
  - The remaining work on this project includes:
    - Installing additional UPS units in closets that were previously unprotected
    - Increasing power coming into the IDF's by working with Morton's Maintenance team in order to ensure sufficient power available for the UPS.
    - Replacing end-of-life UPS batteries in MDF locations to ensure full redundancy and reliability

Professional Development and Certification Update

Professional development continues to be a critical component of strengthening Morton's technology services and ensuring alignment with the district's IT Roadmap Objectives for 2025-2026:

1. **Strengthening Cybersecurity and Data Protection**
2. **Ensure tools "just work" for teaching and learning**
3. **Modernize communication and collaboration**
4. **Streamline operations and service delivery**
5. **Build a culture of continuous improvement**

Over the past six months, IT team members have completed a series of advanced certifications directly tied to these objectives. This strategic alignment ensures the district is investing in skills that improve security, operational reliability, and the overall technology experience for students and staff. The coursework and credentials earned empower our team with additional tools and expertise that directly benefit Morton.

Team Certification Highlights

Yasir Yaseen — Senior Network Administrator

- **Cisco Certified Network Professional (CCNP)**
- **IBM Cybersecurity Architecture**
- **Cisco Network Security**
  These highly specialized credentials provide strategic leadership, enterprise architecture expertise, risk management capability, and governance oversight—supporting all five IT Roadmap Objectives, especially Objective 1 (Strengthen Cybersecurity & Data Protection), Objective 4 (Streamline Operations & Service Delivery), and Objective 5 (Build a Culture of Continuous Improvement).

William Womack — System Administrator

- **Microsoft 365 Certified: Administrator Expert**
- **VMware Certified Professional – Data Center Virtualization (VCP-DCV)**
- **Azure Administrator Associate (AZ-104)**
  William's certifications enhance Morton's cloud management, virtualization, and identity infrastructure—advancing Objective 1 (security), Objective 2 (reliability), and Objective 3 (modern collaboration).

Anthony Figueroa — Junior System Administrator

- **CompTIA A+ 1101**
- **CompTIA A+ 1102**
- **CompTIA Server+**
  These foundational and server-level certifications support Objective 4 (service delivery) and Objective 5 (continuous improvement), and strengthen Morton's technical support and systems management capacity.

Artur Wilczynski — Director of Technology

- **MIT – AI Strategy and Leadership Program: Thriving in the New World**
- **Project Management Professional (PMP)**
- **Certified in the Governance of Enterprise IT (CGEIT)**
- **Certified Information Security Manager (CISM)**
- **Certified in Risk and Information Systems Control (CRISC)**
- **TOGAF Enterprise Architecture Practitioner**

These highly specialized credentials provide strategic leadership, enterprise architecture expertise, risk management capability, and governance oversight—supporting all five IT Roadmap objectives, especially Objective 1 (cybersecurity), Objective 4 (streamlined operations), and Objective 5 (continuous improvement).