# Morton IT Department
# October 2025 Update

## 1. Firewall Upgrade

Over the weekend of September 20–21, the Technology Department completed Phase One of a three-phase firewall modernization plan designed to strengthen Morton's network security, stability, and long-term scalability.

- Phase One, completed in September 2025, laid the foundation for the next stages of the upgrade and resolved several ongoing challenges related to web filtering and VPN connectivity. This foundational phase elevated the district's firewall software to a higher version, providing improved reliability and compatibility with modern tools and configurations.
- Phase Two, scheduled for October 2025, will upgrade Morton to the most up-to-date Cisco firewall firmware available today, along with the latest management dashboard and analytics tools. This phase will deliver enhanced visibility, more precise control of network policies, and stronger cybersecurity capabilities.
- Phase Three, planned for Spring Break 2026, 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. VPN Upgrade

Following the firewall implementation, the district deployed an updated Virtual Private Network (VPN) client for all Morton-issued laptops.

- Deployment has reached 86% of faculty and staff laptops, with the remainder completing automatically when connected to Morton Wi-Fi.
- The new VPN ensures secure off-campus connectivity to district systems, automatically activating when users are outside Morton's network.
- All clients are now required to authenticate through Microsoft Entra ID (Azure) with Multi-Factor Authentication (MFA) before accessing Morton's network.
    - This change significantly increases district security, ensuring that every remote connection is verified and protected.
    - Previously, VPN users connected without authentication, leaving a potential security gap.
- This upgrade provides stronger encryption, improved reliability, and streamlined authentication through Entra ID's centralized identity platform.
- The VPN upgrade also supports Morton's broader cybersecurity initiative by ensuring consistent remote-access security while remaining compatible with individual home internet security tools.
- Prior to this upgrade, some clients experienced conflicts between Morton's VPN and home security software; the new system resolves these issues, enabling a seamless, secure connection regardless of home network configuration.

---

### 3. RingCentral Implementation – 863 Phone Lines Configured

As part of Morton's Unified Communications modernization, the district completed setup of 863 RingCentral phone lines across schools and departments.

- This project was completed in partnership with Blue Wire Communications, ensuring a smooth transition and comprehensive configuration support throughout the process.
- All staff now have direct inward dial (DID) numbers, allowing parents and colleagues to contact staff directly.
- Integration with Microsoft Teams and district voicemail is complete, enabling unified messaging and call routing.
- Hunt groups, front-office routing, and voicemail configurations were standardized for consistent user experience.
- Morton has submitted an application to the FCC for SMS licensing, which will enable secure two-way text messaging through RingCentral in the near future.

## 4. Fall Testing Readiness and Support

On Wednesday, October 1st, all Morton campuses successfully completed Fall Testing, including the administration of the Pre-ACT and Pre-ACT 9 assessments.

- The TestNav platform was deployed to all student devices district-wide in advance of testing.
- Students were able to log in, access, and complete their assessments without appreciable challenges.
- Collaboration between the Technology Department, campus testing coordinators, and the Data Team ensured a smooth, reliable testing experience across all schools.
- System performance and network bandwidth remained stable throughout testing, even during peak utilization periods.

## 5. Mustang Portal – IT Helpdesk Implementation

Mustang Portal, Morton's new online helpdesk system, has been successfully implemented district wide.

- A link to the Mustang Portal was distributed to all Morton devices, giving faculty and staff instant access to the system from their desktops and laptops.
- Phase One of the Mustang Portal project provides faculty and staff the option to enter IT service requests directly instead of going to TSI in person or calling for support.
- Faculty and staff are now entering technology requests and service tickets directly through the portal, allowing the IT team to prioritize and resolve issues more efficiently.
- This system streamlines support workflows, improves ticket tracking, and ensures accountability across IT service areas.
- Phase Two of the rollout will occur in December, empowering students to submit their own requests for assistance.
- The Mustang Portal represents another step toward a more efficient, transparent, and user-friendly technology support environment.

## 6. Cybersecurity Monitoring and Threat Response

Morton now actively utilizes Barracuda Security and Malwarebytes ThreatDown to monitor, detect, and respond to cybersecurity threats across the district's network, devices, and infrastructure.

- These platforms provide real-time visibility, behavioral analytics, and automated threat response, creating multiple layers of protection against phishing, malware, ransomware, and zero-day attacks.
- Barracuda Security focuses on email, web, and network-based threats, while Malwarebytes ThreatDown provides endpoint protection, remediation, and behavioral defense across faculty, staff, and administrative devices.
- Today, the district's cybersecurity focus is on protecting faculty and staff devices, along with core infrastructure hardware such as servers and network appliances, ensuring that foundational systems remain secure and stable.
- Faculty and staff account takeovers have been eliminated due to the successful implementation of Multi-Factor Authentication (MFA) through Microsoft Entra ID (Azure) and continuous monitoring.
- Student account takeovers remain a challenge, as students are not yet required to use MFA; additional safeguards and education initiatives are being developed.
- The IT team continues to monitor system alerts daily, ensuring rapid response and containment to any attempted breaches.

---

## 7. Airtame Platform Adoption

Morton has adopted the Airtame platform district wide as the standard for wireless screen casting and presentation sharing.

- Previously, Airtame was used only for digital signage and hallway TV displays.
- The platform now supports classroom instruction, meeting spaces, and administrative offices for consistent and secure screen sharing.
- This adoption reduces the number of screen-casting platforms from four separate tools down to one unified, secure, and tested solution, simplifying support and improving reliability.
- The district-wide standardization also lays the groundwork for integration with the upcoming Morton Guest Wi-Fi network, planned for Fall 2026, which will extend secure casting capabilities to visitors and students.

- Airtame enables cross-device compatibility for Windows, macOS, and ChromeOS users without cables.
- This adoption provides a scalable, sustainable solution that improves both user experience and device management efficiency.

---

## Next Steps

- Continue monitoring firewall and VPN performance metrics to ensure ongoing stability.
- Complete VPN distribution through Software Center and finalize student-facing documentation.
- Begin Phase 2 of RingCentral deployment to activate text messaging and enhance call-analytics reporting.
- Launch Phase 2 of the Mustang Portal in December to include student service access.
- Expand cybersecurity awareness training and explore the potential adoption of MFA for students to prevent account takeovers and improve overall account security.
- Continue collaboration with the Assessment and Data teams to prepare for Biliteracy Testing and ACCESS Testing this fall and winter.
- SailPoint Identity and Access Management (IAM) will go live in November, integrating with Skyward Academic, Skyward Financial, Microsoft Entra ID (Azure), and RingCentral to automate account provisioning, access control, and lifecycle management.
- Monitor and gather feedback from faculty and administrators on Airtame usability to guide future enhancements.
- Transition Morton's Internet Service Provider (ISP) from AT&T to the Illinois Century Network (ICN) through E-Rate funding.
    - This change will increase Morton's bandwidth from 2 Gbps to 10 Gbps per building, greatly improving network performance, reliability, and scalability.