Strengthening Security at Cardinal Services

At Cardinal Services, protecting client and employee data remains a top priority. Over the past year, we have made significant investments to enhance our security infrastructure, strengthen data protection, and align with evolving industry best practices.

Advanced Threat Monitoring and Endpoint Protection
We have upgraded our endpoint security from traditional EDR to a comprehensive XDR solution, enabling 24/7/365 monitoring across all company computers and servers. This enhancement provides deeper visibility into potential threats and faster response times.

Secure Cloud Infrastructure
All company documents have been migrated to Microsoft 365 cloud storage, protected by strict access controls and multi-factor authentication. In addition, customer records have been transitioned to a secure, cloud-based HCM platform (PrismHR), ensuring sensitive information is managed within a hardened and compliant environment.

Multi-Factor Authentication Across All Systems
We have enforced multi-factor authentication (MFA) across all external platforms, including VPN access. This ensures that all remote and cloud-based access points require an additional layer of verification to protect against unauthorized access.

Enhanced Network Security and Segmentation
To reduce risk from personal devices, we have implemented segmented guest Wi-Fi networks at all office locations. Employees are required to connect personal devices only to these isolated networks, which do not have access to internal systems.

Data Loss Prevention and Cloud Security Controls
We have deployed Data Loss Prevention (DLP) policies across our network and Microsoft 365 environment to prevent unauthorized data sharing or exfiltration. Additionally, Microsoft Defender security services are in place to enforce cloud data protection policies and strengthen our overall security posture.

Secure Remote Access and Vulnerability Management
Remote access has been further secured through VPN multi-factor authentication, along with ongoing vulnerability scanning using Fortinet tools. These controls help identify and address potential risks before they can be exploited.

Email Security and Communication Integrity
To protect communications, we have implemented industry-standard email authentication protocols, including DKIM, SPF, and DMARC. These measures help prevent spoofing and ensure the integrity of email communications.

Comprehensive Security Audit
We completed a thorough audit of all user accounts, hardware, servers, and systems. This review ensured alignment with current security standards and reinforced our commitment to maintaining a secure and compliant environment.

Our Commitment
These enhancements represent a significant step forward in strengthening our security and safeguarding the data entrusted to us. Cardinal Services remains committed to continuous improvement and proactive risk management to ensure the highest level of protection for our clients and their employees.