Action Required:

Update to Transport Layer Security (TLS) Requirements

To enhance security and align with the recent Payment Card Industry Security Standards Council (PCI SSC) updates for migrating from Secure Sockets Layer (SSL) and early versions of Transport Layer Security (TLS), Cardinal is updating its encryption policies.

What does this mean for you?

Today, SSL and early versions of TLS v1.0 no longer meet security standards, because they are vulnerable. According to PCI DSS v3.1, these are not considered strong cryptography and cannot be used as a security control **after June 30, 2018**.

NOTE: *After much feedback, PCI SSC had decided to revise this date from June 30, 2016 to the June 30, 2018, which offers additional time to migrate, but waiting is not recommended due to the vulnerabilities of earlier versions.*

What do I need to do?

PCI recommends that existing implementations be upgraded immediately, as continued use of SSL/early TLS potentially puts the environment at risk. All new implementations must be enabled with TLS v1.1 or greater, although TLS v1.2 is better, and recommended. Your servers need to be updated to accept TLS v1.1 or higher for both inbound and outbound connections.

Cardinal is here to help. If you have any questions regarding this upgrade, email us at issuerservicestech@cardinalcommerce.com.

Your One Connection to Cardinal will FutureProof™ your business.

Contact us at: issuerservicestech@cardinalcommerce.com or visit www.cardinalcommerce.com.