11. Strong Cryptography and Protocols Policy

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Administrative Systems PCI Compliance Services has established a formal policy and supporting procedures concerning the use of strong cryptography and protocols. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Administrative Systems PCI Compliance Services’ needs and goals.

Policy
Administrative Systems PCI Compliance Services will ensure that the use of strong cryptography and protocols adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Use strong cryptography and security protocols (SSL/TLS, IPSEC, SSH, etc.) for safeguarding sensitive cardholder data during transmission over open, public networks.
- Comprehensively document all locations where cardholder data is transmitted or received over open, public networks.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all cardholder data is encrypted with strong cryptography during transit.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only trusted keys and/or certificates are accepted.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the proper encryption strength is implemented for the encryption methodology in use.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that SSL/TLS is enabled whenever cardholder data is transmitted or received.

Responsibility for Policy Maintenance
Administrative Systems PCI Compliance Services is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.