18. Data Control & Access Control Policies

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 data control and access control. 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 Data Control & Access Control policy 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):

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Access needs are to be defined for each respective role, specifically:
    - System components and data resources that each role needs to access for their job function.
    - Level of privilege required for accessing resources.
- Access rights for privileged users are restricted to the least privileges necessary to perform job responsibilities.
- Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC).
- An authorization form is required for all access, which must specify required privileges, and must be signed by management.
- Access control systems are in place on all system components.
- Access control systems are configured to enforce privileges assigned to individuals based on job classification and function.
- Access control systems have a default *Deny All* setting.
- Security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

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.