Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

SECTION 25 – PCI SECURITY POLICIES

Employees of Tyler ISD who receive payments via credit card transactions are expected to comply with best practices for maintaining data security as outlined below. These practices/policies are designed to keep Tyler ISD compliant with Payment Card Industry Data Security Standards.

1.1 - Inventory and physically secure all media that stores confidential information

1.1.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured. Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.

1.2 - Maintain media controls

1.2.1 - Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data.

1.2.1.1 - The organization must ensure all paper and electronic media that contains cardholder data are physically secured. Verify procedures exist for controlling physical access to paper and electronic media, including reports, faxes, CDs, disks, and hard drives.

1.2.1.2 - The organization must ensure any media that contains cardholder data is strictly controlled during any distribution, either internally or externally. Verify a policy exists for the distribution of media containing cardholder data and that the policy covers the distribution to individuals in the organization.

1.2.1.2.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.

1.2.1.2.2 - The organization must maintain control over all media that contains cardholder data. Verify a policy exists for controlling the storage of media containing cardholder data.

1.2.1.2.3 - The organization must ensure all media containing cardholder data is classified as confidential. Ensure all media containing sensitive information is labeled "Confidential."

1.2.1.2.4 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility. Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

1.3 - Label media

1.3.1 - The organization must ensure all media containing cardholder data is classified as confidential. Ensure all media containing sensitive information is labeled "Confidential."

1.4 - Track while in transit

1.4.1 - The organization must ensure all media containing cardholder data can be tracked when being sent outside the facility. Ensure all media containing cardholder data that is sent outside the organization is authorized, logged, and tracked during transit.

1.5 - Obtain management approval for transit

1.5.1 - The organization must ensure procedures are in place to have management approve any transit of sensitive media from a secured area.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

SECTION 25 – PCI SECURITY POLICIES, continued

1.6 - Physical protection while media is in storage

1.6.1 - The organization must maintain control over all media that contains cardholder data. Verify a policy exists for controlling the storage of media containing cardholder data.

1.7 - Manage disposition and destruction

1.7.1 - The organization must ensure all cardholder data is destroyed when it is no longer needed. Verify the media destruction policy covers all types of media that contains cardholder data.

1.7.1.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

1.8 - Destruction and disposal of hard copy materials and media

1.8.1 - The organization will ensure that all hardcopy materials and media to be destroyed are done so in accordance with the strictest standards and guidelines.

1.9 - Management of third party services

1.9.1 - The organization must ensure the service provider policies and procedures includes a list of all service providers, how the organization will monitor the compliance of the service provider with the PCI DSS requirements, and due diligence. Verify all third party service providers have policies and procedures in place requiring a list of all connected entities, performing due diligence prior to connecting the entities, verifying PCI DSS compliance, and for connecting and disconnecting entities.

1.9.1.1 - Maintain a list of service providers. The testing procedures from Appendix A of this document should be performed to ensure the hosting providers are protecting the environment and cardholder data.

1.9.1.2 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.

1.9.1.2.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.

1.9.1.2.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.

1.9.1.2.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

1.9.1.2.2 - Maintain a program to monitor service providers' compliance status.

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

SECTION 25 – PCI SECURITY POLICIES, continued

1.9.1.3 - The organization will maintain a policy, standard, and procedure to select suppliers according to a fair and formal practice to ensure a viable best fit based on requirements.

1.10 - Supplier Interfaces

1.10.1 - Maintain a list of service providers. If these suppliers and service providers touch or use cardholder data, an authorized representative from each service provider should provide attestation of compliance for PCI DSS.

1.11 - Acknowledgment of responsibility for data in possession and control

1.11.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.

1.11.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.

1.11.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

1.12 - Formalize third party relationships

1.12.1 - Establish processes and procedures for engaging service providers, including proper due diligence prior to engagement.

1.12.1.1 - The organization must ensure a written agreement exists stating that the service provider is responsible for all cardholder data that the service provider possesses. Ensure all third party contracts contain a statement requiring the third party to acknowledge its responsibility for the security cardholder data it possesses.

1.12.1.1.1 - Hosting providers must ensure the organization's environment and cardholder data that it is sharing is protected.

1.12.1.1.2 - Shared hosting providers must ensure that only processes that have access to the cardholder data can be executed by that organization and that the organization's access and privileges are restricted to its own cardholder data environment. Verify if shared hosting providers are running their own applications, they are executed with the unique ID of the entity. Verify that any applications used by the hosting provider do not have a privileged user ID; the service provider has only read, write, or execute permissions for files it owns; the service provider's users do not have write access to shared binaries; logs only can be read by the owner of the

Administrators Operating Guide is intended to supplement and define Board policies, serve as administrative regulations and official directives.

SECTION 25 – PCI SECURITY POLICIES, continued

information; and restrictions are in place for disk space, bandwidth, memory, and CPU usage.

1.12.1.2 - Maintain a program to monitor service providers' compliance status.

1.13 - Audit provisions

1.13.1 - Maintain a program to monitor service providers' compliance status.

2.0 Enforcement

Failure to comply with the policies outlined above may result in a failure of the companies PCI compliance and may result in penalties up to termination of the offending employee.