Frankfort Square Park District
Payment Card Industry Data Security Standards Policy

It is the policy of the Frankfort Square Park District to comply with the Payment Card Industry Data Security Standards (PCI-DSS) for the protection and security of payment card information.

The following items are considered specific guidelines associated with this policy and shall be assigned to corresponding procedures as developed.

1. In order to minimize risk, only those data elements on payment card that are needed for District business should be stored.
2. Access to payment card holder data should be limited to District employees requiring such information to complete assigned job tasks.
3. Payment card data on an internet connected computer or processed through the internet, should be protected through a secure network with periodic monitoring of its security.
4. Paper and electronic media that contain card holder data should be physically secure and identifies as confidential information.
5. Payment card data on documents should be redacted, if feasible, when no longer needed for District business. Documents with legible payment care data should be destroyed in accordance with the Local Records Act (50 ILCS 205/1, et. seq.) with appropriate security handling.
6. Security awareness training should be provided for District employees involved in payment card processing.
7. The District should assure that its relationships with payment card service providers comply with PCI-DSS.
8. The District should periodically complete self-assessments of its payment card security systems.
9. The Executive Director should be promptly notified of any information security breach.

_____ _____

Executive Director Date

_____ _____

President Board of Commissioners Date