PCI SECURITY COMPLIANCE POLICY

Geneva Public Library District abides by the following security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program.

1. **Scope of Compliance**
   PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, the Geneva Public Library District cardholder environment consists of four Bibliotheca self-check machines using Comprise SmartTerminal credit card terminals. Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements defined in Self-Assessment Questionnaire C, version 3.0, released February 2014.

2. **Protecting Cardholder Data**
   - The library uses network segmentation and a stateful packet inspection firewall to prohibit public access to the cardholder environment.
   - The library allows vendor access to the cardholder environment only during time needed and monitors such access via firewall logging.
   - The library maintains the physical security of the cardholder environment by utilizing locks on-network cables and password protecting the self check machines and SmartTerminal credit card terminals.
   - The library does not store credit card data of any kind.
   - Transmission of cardholder data is encrypted via Magtek SmartTerminal card readers that utilize a PCI DSS compliant security architecture.

3. **Security Practices**
   - The Library performs quarterly security scans through Trustwave, Inc. to ensure continuing PCI compliance. Scan logs are kept for a period of one year.
   - The Library maintains a list of serial numbers for devices used. The self-check machines and SmartTerminal card readers are inspected for tampering on a monthly basis.
• The Library requires verification of third party vendors and service personnel.
• Library staff is trained annually in the importance of cardholder data security and security procedures.
• In the event of a security incident, Library personnel will coordinate with the merchant bank, relevant credit card companies, and law enforcement. Persons with information compromised by a data breach will be notified in accordance with federal and state law.

Rev. 2.27.20