EXHIBIT A

City of Rio Rancho, New Mexico
Credit Card and Electronic Payment Acceptance Policy

Purpose. The purpose of this policy is to provide guidance for accepting credit/debit card payments or electronic transfers. Section 6-10-1.2 NMSA 1978 provides that a local governing body may accept payment by credit card or electronic means and may charge a uniform convenience fee to cover the approximate costs imposed by a financial institution that are directly related to processing a credit card or electronic transfers.

Scope. This policy applies to all departments that accept or may in the future accept credit cards or electronic transfers for payment of goods and services. All City employees involved in electronic transfers or processing credit card transactions and in the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) are subject to the terms of this policy.

Acceptance and Processing. Credit card payments shall be used for the sole purpose of processing payment transactions for goods and services provided by the City of Rio Rancho to the cardholder. Cash advances or cash withdrawals are not authorized at the City of Rio Rancho and will not be processed. In addition, the City of Rio Rancho will assess a convenience fee as stipulated below:

1. Except when credit card or electronic payment processing fees are included in the fee charged for a specific service, a convenience fee of $1.75 will be added for credit card and electronic forms of payment processed by the City of Rio Rancho excluding payments transacted within copy machines and printers at City library facilities where transaction sizes are usually minimal and the fee would impose an undue burden on the cardholder, or where otherwise prohibited by law or under any agreement with the payment processor.

   The convenience fee for the City or individual departments may change in the future. The convenience fee and the methodology used in calculating it must be in accordance with the contracts the City of Rio Rancho has established with its payment processing vendors.

Handling Credit Card Information. Technology implementation must follow industry guidance, procedures, and rule compliance established by the National Automated Clearing House Association (NACHA) for electronic payments and Payment Card Industry Data Security Standards (PCI DSS) for credit card payments. In accordance with PCI DSS, Req. 12.6.1, all employees involved in processing credit card transactions and the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) must be trained upon hire.

Protecting cardholder data is essential thus every effort shall be made to protect such information. Any physical access to cardholder information will be appropriately restricted to data or systems that house, process, or transmit cardholder data in such a manner as not to allow the opportunity for persons to access or remove devices, data, or systems.

For each payment channel the acceptable PCI DSS compliance method is explained below:

1. **Via the internet:** Transactions can be processed through the existing secured websites provided by the City of Rio Rancho as well as any other payment option that is implemented by the Financial Services and Information Technology Departments. The websites contracted by the City must follow industry compliant protocols and procedures.

2. **Via the phone:** Staff can take credit card payments over the phone provided they have been trained on safe procedures. Credit card information shall be entered directly into the payment processing system only. Credit card information shall not be recorded in writing under any circumstance. Customers can also pay over the phone by using the Interactive Voice Response (IVR) system which provides a secure payment processing option.

3. **Via U.S. Mail:** Whenever a payment is received by US mail, the form containing the credit card information must be shredded. Staff shall be trained to safely and expeditiously discard any personal information.

4. **In person:** All in-person credit card transactions must be processed while the customer is present and in full view of the customer. Staff is prohibited from writing or storing credit card information. Security controls must be in place when handling in-person transactions.

5. **Via Fax or Email:** Credit card information cannot be accepted via fax or email or any other unsecure communication medium. If a customer does send an email with their card information, it must be deleted immediately from all email folders. The customer shall also be contacted to indicate that the information has been deleted and the transaction has not been processed. The staff member may then work with the customer to complete the transaction in an authorized manner.

Accounting Controls. Each day the cash receipts batches must be closed and reconciled by the cashiers. A detailed reconciliation process will be performed daily by the Financial Services Department after which the batches will be posted into the financial system. All batch copies shall be retained for audit purposes.

Payment Card Industry Data Security Standards. The PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. Noncompliance to these standards may result in loss of the ability to accept credit cards.

In order to ensure compliance with PCI DSS requirements an annual PCI Self-Assessment Questionnaire must be completed and submitted to DFA annually. All standards for the PCI DDS requirements can be found at https://www.pcisecuritystandards.org/

Contracts. The Financial Services Department shall establish and administer contracts with vendors for the acceptance and processing of credit card payments, including, but not limited to internet payment gateway services and third party electronic payment processors. The City will pay all costs associated with the acceptance of payment card services, including purchases or leases of merchant equipment as set out in the Fiscal Agent Agreement and any agreement with an approved third-party processor and any assessment charged to cover the costs of compliance with PCI DSS and NACHA.

Effective Date. This policy will take effect the later of September 1, 2022 or when necessary technology can be obtained and implemented.