"Exhibit A"

COMPUTER FRAUD PREVENTION POLICY

Adopted February 10, 2020; Amended 9-14-2021

I. Establishing New ACH Accounts

New vendors requesting payment by ACH should return the ACH payment request form with their W9 form and first invoice. Forms should accompany a copy of a voided check or a letter from the financial institution where the account is held. Vendor contact information on the form will be cross-referenced with contact information currently on file with the purchasing office or accounts payable. The supervisor of the employee processing a new ACH account shall review and approve all applications prior to the account being opened.

II. Making Revisions to Existing ACH Accounts

Vendors requesting to make changes to ACH instructions currently on file will also be requested to supply the information currently on file as a double-check. Email requests will be followed up with a phone call to the phone number currently on file with purchasing or accounts payable, and not the phone number or email address supplied with the request. This is to ensure that the request came from the vendor and not a fraudulent email address. The supervisor of the employee making revisions to an existing ACH account shall review and approve all changes prior to final implementation.

III. Investigating Suspicious E-Mail Addresses

If uncertain if a vendor's email address is fraudulent, we should investigate previous emails/invoices from the vendor and/or have the IT staff or contractor review the email string to evaluate the validity of the address.

IV. Anti-fraud Training

Employees responsible for processing wire transfers shall be provided anti-fraud training, including but not limited to detection of social engineering, phishing, business email compromise, and other scams.

V. Confirmation of Wire Transfer Requests

Internal requests for wire transfers shall be confirmed by another means other than the one originally used to make the request.