Policy No. 19

Fraud Prevention and Response Protocols

Fraud Prevention Measures:

1. Keep contact information with banks up to date
    - CFO is the primary administrator and point of contact for all EDC bank accounts.
    - When staff/board/committee members turnover, updating this information is a priority

2. Create strong passwords, change them periodically and do not share them.

3. Enable alerts for bank activity.

4. Use only protected devices for online banking activity.

5. When eligible, enable 2-factor identification to log into accounts and to approve transactions.

6. Use internal 2-person approval for all transactions.

7. Know which third parties have access to our account information.

8. Stay current with bank activity - log into online bank accounts twice (2x) per week.

9. Meet annually with bank reps both to update contact information and be educated about the latest scam schemes and fraud protection services.

Fraud Activity Response Protocols:

1. Prepare a hard copy (directly printed from online banking platform) of suspicious transactions making sure to include a record of the last legitimate transactions.

2. Confirm with other account administrators that activity is unfounded.

3. Contact bank rep (@GFNB Megan Bohan 518-415-4519) to conduct an immediate investigation in the activity.

4. Have accounts frozen until nature of the suspicious activity is identified.

5. Contact EDC-CEO (Jim Siplon) and EDC Board Chair (Mitch Amado) to inform them of the situation and continue to keep them updated with developments.

6. If fraud activity is conclusive, close accounts and have funds transferred to new accounts.

7. Notify vendors – all outstanding checks will need to be voided and re-issued.

8. Debrief with bank reps and relay information to EDC Board of Directors.

9. Complete necessary paperwork and orders for new checks and deposit slips.

Adopted October, 18,2022

Re-Affirmed March 21, 2023
Re-Affirmed March 20, 2024